ESCUELA POLITÉCNICA SUPERIOR
INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

PROYECTO FIN DE CARRERA

Definición de un marco de trabajo basado en CObIT para la auditoría de TI en un bufete

Autor: Nicolás Palmer Vallée

Tutor: Ana Isabel González-Tablas

Leganés, Octubre de 2015

Título: Definición de un marco de trabajo basado en CObIT para la auditoría de TI en un bufete

Autor: Nicolás Palmer Vallée

Director: Miguel Ángel Ramos González

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día 22 de Octubre de 2015 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

A mi pareja y mis padres, por su apoyo, sus palabras de ánimo y por no darme por imposible.

A mis tutores y profesores Antonio G. Carmona, Miguel Ángel Ramos y Anabel por todo el tiempo dedicado y su dedicación a ayudarme en la finalización de este proyecto. Por la paciencia mostrada a cada toma de contacto con ellos y por sus ánimos, gracias a los cuales he logrado finalizar dicho proyecto.

Resumen

El presente Proyecto versa sobre la realización de una Auditoría de Sistemas de la Información (SI) en un Bufete de abogados de tamaño medio (unas 20 personas). Tal como explicaré en el desarrollo del Proyecto, existen diversos tipos de Auditoría, pero considerando mi formación académica, así como mi experiencia profesional como Helpdesk en dicha empresa, he centrado el mismo en la ejecución de una Auditoría Informática.

En este tipo de empresas, los procesos TI no se encuentran generalmente sometidos a un protocolo corporativo, ni se trata de sistemas muy metódicos, lo que conlleva la existencia de errores en datos, fallos en la infraestructura TI y graves consecuencias económicas.

Mi intención, apoyándome en la metodología CObIT, y dada la trascendencia económica y social de las Pequeñas y Medianas Empresas en el tejido empresarial del país, es la de diseñar un proceso, conformado por hitos o etapas cuantificables que pueda ser seguido por un auditor informático, a fin de determinar el nivel de gestión de los SI en cualquier Pyme, como por ejemplo, además del presente caso, un estudio de arquitectura, una Gestoría, un Departamento de RR.HH., etc.

Palabras clave: auditoría informática, CObIT, buenas prácticas, PyME, checklist, Sistemas de la Información, Tecnologías de la Información.

Abstract

This Final Degree Project (Thesis) is about the execution of an IS audit over a medium size lawyer's office. As I will explain during the development of the document, there are different types of audit, but considering my academic education and my professional experience as helpdesk within the company, I've focused the project on the execution of an Information System audit.

In this kind of company, the IT processes neither are usually subject to a corporate protocol, nor to a methodical system of IT managing. This situation can leads to many data errors, failures on the IT infrastructure and serious economic consequences.

My intention is to design a CObIT-methodology-based process comprising measurable milestones or steps that can be followed by an IS auditor in order to evaluate the level of IS management within any SME, like an architecture firm, an agency, a HR department or, the present study case, a lawyer's office.

Keywords: IT audit, CObIT, good practices, SME, checklist, System of Information, Information Technologies.

Indice

1.- Introducción 1
Motivación 1
Objetivos 2
Estructura de la memoria 2
2.- Estado del arte 3
Definición de auditoría de los Sistema de la Información - ¿Qué es? 3
Necesidad de una auditoría informática – Objetivos 5
Perfil del auditor informático 6
Ámbito de aplicación de auditoría informática 9
Tipos de auditoría informática 11
¿Qué es CObIT? 13
Legislación aplicable 19
L.O.P.D. 19
L.S.S.I. 20
Ley de Propiedad Intelectual 21
3.- Análisis de la situación 23
Estructura del proyecto 23
TI en un bufete 24
Razones para una auditoría informática 25
CObIT 25
I - Planear y organizar 27
1.- Definir un plan estratégico de TI – PO1 27

2.- Definir la arquitectura de información – PO2 28
3.- Administrar la Inversión en TI – PO5 29
4.- Administrar los recursos humanos de TI – PO7 30
5.- Evaluar y administrar los riesgos de TI – PO9 31
6.- Administrar proyectos – PO10 32
II - Adquisición e implementación 34
1.- Identificar soluciones automatizadas – AI1 34
2.- Adquirir y mantener software aplicativo – AI2 34
3.- Adquirir y mantener infraestructura tecnológica – AI3 35
4.- Facilitar la operación y el uso – AI4 37
5.- Adquirir recursos de TI – AI5 38
III - Entregar y dar soporte 39
1.- Definir y administrar niveles de servicio – DS1 39
2.- Administrar los servicios de terceros – DS2 40
3.- Administrar el desempeño y la capacidad – DS3 41
4.- Garantizar la continuidad del servicio – DS4 41
5.- Garantizar la seguridad de los sistemas – DS5 44
6.- Educar y entrenar a los usuarios – DS7 45
7.- Administrar la mesa de servicio y los incidentes – DS8 47
8.- Administración de los datos – DS11 48
9.- Administración del ambiente físico – DS12 49
10.- Administración de operaciones – DS13 50
IV - Monitorear y evaluar 51
1.- Monitorear y evaluar el desempeño de TI – ME1 51
2.- Garantizar el cumplimiento regulatorio – ME3 52
4.- Elaboración de un marco de trabajo basado en CObIT 54

Alcance de la auditoría 54
Dimensionamiento 54
Operativa del bufete 55
Infraestructura TIC 55
Alcance de la ASI 57
Objetivos del Dpto. TI 57
Base de análisis y controles 58
Selección de procesos CObIT 59
Proceso PO1 60
Proceso PO2 61
Proceso PO5 61
Proceso PO7 62
Proceso PO9 63
Proceso PO10 63
Proceso AI1 64
Proceso AI2 65
Proceso AI3 66
Proceso AI4 67
Proceso AI5 68
Proceso DS1 69
Proceso DS2 70
Proceso DS3 71
Proceso DS4 72
Proceso DS5 73
Proceso DS7 74
Proceso DS8 76

Proceso DS11 78
Proceso DS12 81
Proceso DS13 83
Proceso ME1 85
Proceso ME3 86
Gráficas de análisis 88
5.- Gestión del Proyecto 90
Gestión del proyecto 91
Diagrama de Gantt 93
Análisis de costes 94
6.- Conclusiones y líneas futuras 97
Conclusiones 97
Líneas futuras 98
ANEXOS 100
Anexo I: L.O.P.D. 100
1.- Política de privacidad 100
2.- Calidad de los datos 101
3.- Deber de secreto 102
4.- Cesión y transferencia de datos 103
5.- Inscripción de los ficheros 104
6.- Derecho de acceso a ficheros 105
7.- Documento de seguridad 106
8.- Medidas de seguridad 106
9.- Niveles de seguridad 106
Anexo II: L.S.S.I.C.E 111
1.- Aviso Legal 111

2.- Política de cookies....112

3.- Comunicaciones comerciales a través de correo electrónico....113

4.- Registro del dominio web....114

5.- Enlaces externos....115

Anexo III: Glosario....115

Anexo IV: Bibliografía....116

Anexo V: Referencias....117

Indice de tablas

Tabla 1- Proceso PO1 27
Tabla 2 - Proceso PO2 28
Tabla 3 - Proceso PO5 29
Tabla 4 - Proceso PO7 31
Tabla 5 - Proceso PO9 32
Tabla 6 - Proceso PO10 33
Tabla 7 - Proceso AI1 34
Tabla 8 - Proceso AI2 35
Tabla 9 - Proceso AI3 36
Tabla 10 - Proceso AI4 37
Tabla 11 - Proceso AI5 38
Tabla 12 - Proceso DS1 40
Tabla 13 - Proceso DS2 40
Tabla 14 - Proceso DS3 41
Tabla 15 – Proceso DS4 43
Tabla 16 - Proceso DS5 45
Tabla 17 - Proceso DS7 46
Tabla 18 - Proceso DS8 48
Tabla 19 - Proceso DS11 49
Tabla 20 - Proceso DS12 50
Tabla 21 - Proceso DS13 51
Tabla 22 - Proceso ME1 52
Tabla 23 - Proceso ME3 53
Tabla 24 - Cuestionario PO1 60
Tabla 25 - Cuestionario PO2 61
Tabla 26 - Cuestionario PO5 62
Tabla 27 - Cuestionario PO7 62
Tabla 28 - Cuestionario PO9 63
Tabla 29 - Cuestionario PO10 64

Tabla 30 - Cuestionario AI1 65
Tabla 31 - Cuestionario AI2 65
Tabla 32 - Cuestionario AI3 66
Tabla 33 - Cuestionario AI4 67
Tabla 34 - Cuestionario AI5 68
Tabla 35 - Cuestionario DS1 69
Tabla 36 - Cuestionario DS2 70
Tabla 37 - Cuestionario DS3 71
Tabla 38 - Cuestionario DS4 72
Tabla 39 - Cuestionario DS5 74
Tabla 40 - Cuestionario DS7 75
Tabla 41 - Cuestionario DS8 77
Tabla 42 - Cuestionario DS11 80
Tabla 43 - Cuestionario DS12 82
Tabla 44 - Cuestionario DS13 84
Tabla 45 - Cuestionario ME1 85
Tabla 46 - Cuestionario ME3 87
Tabla 47 - Calendario del proyecto 94
Tabla 48 - Coste personal 95
Tabla 49 - Gastos SI 95
Tabla 50 - Presupuesto final PFC 96

Indice de figuras

Figura 1 - Valores éticos del auditor 9
Figura 2 - Conceptos y relaciones de seguridad TI 11
Figura 3 - Legislación española 12
Figura 4 - Tipos de ASI 13
Figura 5 – Áreas de enfoque del Gobierno TI 14
Figura 6 - Estructura de CObIT 16
Figura 7 – Cubo de CObIT 17
Figura 8 – Marco de trabajo CObIT 18
Figura 9 - Marco Organizativo 54
Figura 10 - Estructura TIC del bufete 56
Figura 11 - Flujo de datos en el despacho 79
Figura 12 - Diagrama de Gantt 93

Indice de gráficas

Gráfica 1 - Métricas de DS8 89
Gráfica 2 - Métricas de AI4 89

1.- Introducción

Motivación

La motivación que me ha llevado a realizar este proyecto de fin de carrera fue el tiempo que estuve trabajando como becario del departamento de soporte técnico de un bufete de abogados. Al principio no le presté demasiada atención debido a que eran mis primeros días de trabajo en la vida real, pero poco a poco me fui dando cuenta de la falta de seguridad respecto a las TI.

Por desgracia, durante esos meses trabajando como *Helpdesk*, me di cuenta de lo mucho que dependen las empresas (de cualquier tamaño) del soporte que les brindan las TI y de la poca conciencia que se tiene de esta misma dependencia. Del mismo modo, existe muy poca conciencia de la necesidad de una correcta supervisión y mantenimiento de estos servicios y hasta que algo no falla, nadie cae en la cuenta de lo relativamente barato que habría costado tener un mantenimiento previo y de lo caro que resulta solucionar un problema.

Frases o excusas como "…*es que siempre lo hemos hecho así*…" o "…*hasta ahora nunca hemos tenido problemas*…" son una clara señal de esa dejadez que puede repercutir en graves problemas tanto económicos como legales para la empresa.

Por todo esto, pienso firmemente que uno de los principales problemas a los que se enfrenta la auditoría informática en el negocio, es la lucha entre "lo que se debería hacer" frente a "lo que cuestan esas medidas". En segundo plano está el factor humano, tal como la dejadez de los empleados a la hora de poner en marcha las medidas de seguridad o como la poca visión de futuro que tienen los responsables de la relación entre el negocio y TI a la hora de desarrollar estrategias de seguridad como copias de seguridad, deslocalización de servidores, etc.

Como ya apuntaba anteriormente, es muy importante la presencia de la PyME en España. Según el informe de la *Ipyme* [*pyme15*] [*epyme14*], el 99,88% del tejido empresarial está constituido por este tipo de empresa, por lo que considero se trata de un sector importante a tratar en lo relativo a las TIC. Y más aún, cuando las cifras del informe del ONTSI [*ontsi*] no presenta cifras muy halagüeñas con respecto a la penetración de las TIC en estas empresas. El uso de las TIC en las PYME's españolas está creciendo [*artmun*], con un tímido avance de los servicios *cloud*, pero aún queda bastante camino por recorrer. De estos datos, me gustaría sacar la conclusión de que es aún más importante que la presencia de las TIC en una empresa no frene su avance, ni suponga un impedimento en las tareas de

sus empleados, sino que se consideren como una herramienta más. Así mismo, puesto que no es muy alto el porcentaje de empresas "tecnológicas", es aún más importante destacar por encima de las otras mediante un gobierno de las TI de calidad.

Objetivos

El fin de este proyecto, tras el análisis del funcionamiento de TI en un bufete, es la realización de un *check-list* o lista de tareas, para realizar una concienzuda auditoría informática lo más extensa posible. Esta lista de tareas da lugar a una "hoja de ruta" que se generará a partir de las recomendaciones surgidas de la auditoría. Por "hoja de ruta", me refiero a una serie de pasos y acciones a tomar para la mejora de los procesos TI del negocio. ¿Cuáles serían los beneficios para el bufete tras la realización de estas acciones? Quizá la obtención de una norma ISO sería apuntar muy alto, sin embargo, podría obtener un sello de calidad específico para las TIC en bufetes gracias al cual pudiera desmarcarse del resto de competidores del sector. Debido a la gran presencia de pequeños y medianos bufetes, considero que esta distinción sería una gran característica diferenciadora en el ámbito del derecho.

Estructura de la memoria

La memoria se compone de tres grandes bloques, identificados por secciones. El objetivo de la primera sección es presentar el mundo de la auditoría informática al lector, describiendo los motivos por los cuales una empresa puede necesitar o requerir los servicios de un auditor. Se presentan las características que ha de cumplir un profesional de la auditoría informática, así como los distintos campos que puede abarcar la auditoría. Se presenta la legislación aplicable al mundo de las TI. Y para completar este bloque, y dado que el objetivo final de este proyecto es la creación de una hoja de ruta de audición basada en ***C****ontrol* ***Ob****ectives for* ***I****nformation and related* ***T****echnology* (CObIT) , paso a explicar y describir qué es y cómo funciona dentro de una empresa y porqué es útil para compañías de este tamaño.

La segunda sección empieza con una descripción del estado de las TI en un bufete de tamaño medio, y de las razones que pueden llevar a realizar una auditoría informática sobre este panorama. La sección se centra a continuación en la metodología CObIT [*cobit*] y sus procesos. Dado que no todas las empresas son iguales por su tipología, dimensiones y naturaleza del negocio, he tomado la decisión de

tomar en consideración aquellos procesos de CObIT que podían ser aplicables a una empresa de este tipo como la que nos ocupa. Por lo tanto, a lo largo de esta sección, detallo los procesos que voy a emplear para definir la auditoría a seguir. Y dentro de cada proceso, elijo los puntos de control que he estimado como los más apropiados para el bufete. Todo eso para los cuatro dominios que conforman la metodología CObIT.

La tercera sección se centra en la aplicación de CObIT y otras metodologías que permitan crear un plan de auditoría informática centrado en la gestión de las TI en un bufete. La idea es que este resultado sirva de guía a un futuro auditor informático para analizar y evaluar la gestión, el funcionamiento y el uso de las TI en un bufete de estas características

2.- Estado del arte

Definición de auditoría de los Sistema de la Información - ¿Qué es?

ISACA (*Information Systems Audit and Control Association*) define la auditoría como *la inspección formal y comprobación de que se están aplicando los estándares y metodologías o que los objetivos de eficiencia o eficacia se cumplan.*

Existen varias definiciones de auditoría de SI [*ai_upv*]:

- La **Norma ANSI N45.2.10.197** la determina como *actividad para determinar por medio de la investigación, la adecuación de y la adhesión a, los procedimientos establecidos, instrucciones, especificaciones, códigos y estándares, u otros requisitos aplicables contractuales o de licencia, así como la eficacia de su implantación.*
- **Acha Iturmendi**, en la publicación "***Auditoría Informática de la Empresa***" la define como *conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existentes en cada empresa, y para conseguir la eficiencia exigida en el marco de la organización correspondiente.*
- Otra definición proveniente de **Alonso Rivas "*Auditoría Informática***" presenta la Auditoría de Sistemas de la Información (ASI) como *un examen metódico del servicio informático, o de un sistema informático en particular, realizado de forma puntual y de modo discontinuo, a*

instancias de la Dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del servicio, o del sistema, que resultan auditados.

Tras analizar todas estas definiciones, si se me permite opinar, entiendo la auditoría informática como el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los objetivos del negocio, utiliza los recursos prestados de forma eficiente y cumple con las leyes y regulaciones existentes aplicables a los SI. Hay que explicar que la realización de una auditoría en una empresa, no implica la existencia previa de problemas. Se puede dar el caso de que un proceso automatizado se esté realizando de forma correcta (con una calificación de 5 sobre 10), pero tras presentar el resultado de la auditoría, que son las recomendaciones por parte del auditor, a la gerencia del negocio, se puede mejorar este proceso consiguiendo que su eficiencia se vea incrementada y pase a realizarse de forma óptima (con una calificación de 8 sobre 10). Durante una auditoría informática, se analiza el uso y la forma de gestionar los servicios y recursos de TI de la empresa para determinar si son adecuados o cumplen sus objetivos. En caso de no hacer correctamente su función se establecerán unos cambios para aplicar. Dado que se trata de una auditoría informática, se analizan los sistemas de la información empezando por las entradas de datos, procedimientos, archivos, seguridad y la obtención de información, y terminando por los elementos de control, de los tres tipos existentes: preventivos, de detección y correctivos, así como los de recuperación tras cualquier contingencia.

Además de la auditoría informática, existen otros tipos de auditorías tales como la financiera cuya misión es evaluar las cuentas de la empresa y presentar la realidad de éstas; la de gestión cuyo objetivo es la dirección del negocio y el análisis de su eficacia, eficiencia y economía. O la operacional, entre otras, cuyo objetivo es el análisis de una organización, departamento o función interna para determinar si se están cumpliendo correctamente los objetivos establecidos por la Dirección.

En muchas ocasiones ocurre que las auditorías se ven como algo negativo por parte del negocio, se ve como un análisis crítico y negativo, como una penalización, además de un gasto extra que hay que afrontar. Hay que ver más allá de estos puntos, a priori negativos y convertirlos en algo bueno y provechoso para la continuidad del negocio aprovechando las recomendaciones que realice el equipo auditor e implementarlas. De esta forma, me gustaría desterrar esa idea generalizada que se tiene sobre la auditoría y los auditores como algo negativo y plantearlo como algo provechoso para la empresa y los empleados.

No quiero dejar pasar este punto sin mencionar la diferencia entre una auditoría informática y una auditoría realizada con elementos informáticos. En el segundo tipo de auditoría se emplean los elementos informáticos como meras herramientas del auditor, igual que un mecánico emplea llaves Allen o dinamométricas para su labor diaria; y una auditoría informática realiza la auditoría (seguramente mediante herramientas informáticas) de toda la infraestructura de SI de la empresa auditada. [*ai_si*]

Otro aspecto en el que quiero hacer énfasis es la diferencia que hay entre "auditoría informática" y "auditoría de seguridad informática", no es lo mismo. Dentro del concepto de "Auditoría Informática", se puede incluir la "auditoría de la seguridad informática", pero también puede coexistir con la "Auditoría de los datos" o la "Auditoría de los recursos TI" entre otros. Es un concepto que en varias ocasiones he tenido que explicar a la hora de hablar con amigos o conocidos acerca de este proyecto.

Necesidad de una auditoría informática – Objetivos

Cada vez más, las tecnologías de la información forman un pilar importante en el soporte del negocio de la empresa y se hacen necesarias las auditorías informáticas. Las necesidades básicas de una auditoría son la función informática, que engloba el análisis de la organización, su seguridad, la segregación de funciones según el personal y la gestión de las actividades de proceso de datos. Los datos, como todos sabemos, suponen uno de los elementos claves en la existencia y desarrollo del negocio. Por otra parte, los sistemas informáticos cuya finalidad es la de asegurar la adecuación de los datos a los fines para los cuales fueron diseñados, también son el objetivo de una auditoría.

Como principales objetivos, tenemos:

- Asegurar a la dirección del negocio y al resto de áreas de la empresa que la información que les llega es la necesaria en el momento oportuno, y es fiable para tomar decisiones estratégicas.
- La eliminación o reducción al máximo de la posibilidad de la pérdida de información por fallos en la infraestructura, en los procesos o por una gestión errónea de los datos.
- Comprobar la seguridad de la información mediante la detección y prevención de fraudes por manipulación de dicha información o por acceso de personas no autorizadas a operaciones transaccionales de datos.
- Verificar que se estén cumpliendo las leyes y regulaciones referentes al tratamiento y gestión de información sensible.

- La relación con empresas proveedoras externas se mantiene según lo pactado.

La realización de una auditoría informática puede usarse para obtener certificaciones oficiales, tales como la ISO 20000 o ISO 27000, que otorguen un sello de calidad a la empresa certificando su correcto funcionamiento interno en lo referente a las TI y SI. Pero no hay que circunscribir la auditoría informática a la seguridad informática, sino también al control de procedimientos, procesos e integridad de la información de forma que se alineen con el negocio.

Perfil del auditor informático

Debido a la naturaleza del proceso auditor, definir cuál ha de ser el perfil del auditor informático se antoja algo complicado. Se podría decir que existen dos vertientes, o dos opiniones al respecto. Como ya hemos explicado anteriormente, y simplificando, la auditoría informática es el análisis y evaluación de los SI de una empresa para lograr el buen funcionamiento de ésta. Con lo cual, se requieren conocimientos técnicos informáticos, pero por otra parte hay que entender la corriente organizativa de la compañía. Así que por una parte está la opinión de que el auditor informático ha de tener una formación técnica, proviniendo de alguna Ingeniería Informática; y por otra parte, la opción de que el auditor sea alguien con formación empresarial, que comprenda bien el concepto del negocio. ¿Cuál prevalece sobre cuál? El auditor informático (en adelante *auditor)* es el encargado de la verificación y certificación del correcto funcionamiento de los SI dentro del negocio, así como quien tiene acceso a datos de la empresa, en ocasiones datos sensibles. Debido a la delicada tarea a la que se enfrenta el auditor (o el grupo de auditores), se han de cumplir ciertas características personales y profesionales para llevar a buen término esta operación [*ai_enf_pract*]:

- **Calidad de trabajo**: el auditor ha de prestar sus servicios según las posibilidades de la ciencia y los medios a su alcance, y en caso de precariedad de medios, deberá negarse a la realización de la auditoría hasta que se garantice un mínimo de calidad exigible. En un momento puntual, podrá solicitar un informe técnico a personal más cualificado que él para asegurar el correcto resultado de la auditoría.
- **Plena capacidad del auditor** para realizar la auditoría solicitada, así como la mejora paralela de sus conocimientos en función de la evolución las TI.
- **Profesionalidad** del auditor: profesionalidad y trato personal correcto de forma que evite caer en exageraciones o atemorizar innecesariamente al auditado. Deberá transmitir una imagen de

precisión y exactitud en sus comentarios e informes. Asimismo, deberá evitar que el exceso de trabajo merme sus posibilidades de concentración y precisión en sus tareas y no aceptar más carga de trabajo en caso de no disponer de tiempo para desempeñar más labores.

- **Concentración en el trabajo:** evitar que el exceso de trabajo pueda mermar la calidad y precisión de su labor y evitar la reproducción de otros trabajos, aunque sí podrá usarlos para contrastarlos con el suyo propio.
- **Confianza:** el comportamiento del auditor ha de transmitir confianza al auditado así como emplear un lenguaje que sea comprensible por el personal del negocio que no tiene porqué ser técnico. Por otra parte, debe existir una clara disposición por ambas partes para el diálogo y el intercambio de opiniones. El auditor ha de aceptar las indicaciones del auditado como válidas, sin dudar de ellas a menos que se presenten pruebas contradictorias.
- **Criterio propio**: el auditor debe actuar libremente y sin coacción, según su saber y su entendimiento. Ha de poder presentar sus pruebas, aun existiendo divergencias de criterios con otros profesionales, que serán reflejadas en el informe final. Tiene que evitar subordinarse y plantearse la continuidad de su relación con el auditado en caso de que éste no acepte sus recomendaciones.
- **Secreto profesional**: puesto que durante su trabajo, el auditor puede llegar a tener acceso a datos sensibles del negocio, no puede difundir esta información a terceros. Y se han de establecer medidas de seguridad por las cuales se asegure al auditado que la documentación generada durante la audición va a quedar almacenada en un entorno seguro y fiable y protegido del acceso no autorizado. Ha de mantener la discreción en la divulgación de los datos para evitar dañar la intimidad o profesionalidad de las personas auditadas. al criterio de otros profesionales, aunque debe saber aceptar las críticas de terceros y analizarlas.
- **No Injerencia**: el auditor debe evitar emitir comentarios sobre el trabajo de los empleados de la empresa, pudiéndose interpretar como despreciativos. Todos aquellos elementos de la infraestructura T.I. de la empresa utilizados para la auditoría, deben permanecer inalterados. La acción del auditor debe ser transparente para los empleados.
- **Cautela**: debido a que el auditor tiene la capacidad de ofrecer al cliente una serie de medidas que tomar para mejorar su negocio, ha de tener sumo cuidado en basar estas sugerencias en más que meras intuiciones obtenidas de la auditoría.
- **Integridad moral**: los principios de integridad moral del auditor deben ser la honestidad, la lealtad y la diligencia en el ejercicio de su labor. Tiene que ceñirse a las leyes concernientes a

las T.I. así como no participar en actos corruptivos. No puede utilizar los datos obtenidos durante la auditoría para sacar provecho propio o perjudicar a la empresa auditada.

- **Economía**: durante el proceso auditor, el profesional evitará generar gastos innecesarios. Se tendrán en cuenta los recursos disponibles y, en caso de necesitar usar recursos compartidos con el personal de la empresa, elegirá el momento en que no se utilicen para interferir lo menos posible en el desarrollo del Negocio.
- **Formación continuada**: dado que las TIC evolucionan constantemente, el auditor está obligado a evolucionar sus conocimientos sobre los SI.
- **Fortalecimiento y respeto de la profesión**: promover el reconocimiento a la labor del auditor y del valor de su trabajo como un valor añadido a la compañía auditada. Evitar la competencia desleal, denunciar comportamientos indebidos y asegurar una remuneración acorde a sus conocimientos y su buen hacer.
- Como punto final: **obtener el beneficio del auditado**. El fin del auditor es el de la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada.

Además de los factores personales, el auditor dispone de varias herramientas que le ayudan y guían a la hora de realizar su labor y de las cuales puede inspirarse. Por una parte ITIL (Biblioteca de Infraestructura de Tecnologías de la Información) es un conjunto de buenas prácticas cuya finalidad es la de mejorar la calidad de los servicios TI. El auditor puede ayudarse de la documentación ofrecida en los libros que componen ITIL [*itil*] para sugerir mejoras en los procesos TI. El CMMI es un modelo para la mejora y evaluación, gracias a una serie de buenas prácticas, de los procesos para el desarrollo, mantenimiento y operación de sistemas de Software. Aunque CMMI no puede emplearse para certificar la madurez de una empresa a este respecto, se recurre a métodos de evaluación tales como SCAMPI. Y finalmente, CObIT, un conjunto de buenas prácticas, recogidas a través de una serie de objetivos de control, que el auditor puede emplear para evaluar el correcto funcionamiento de TI del negocio.

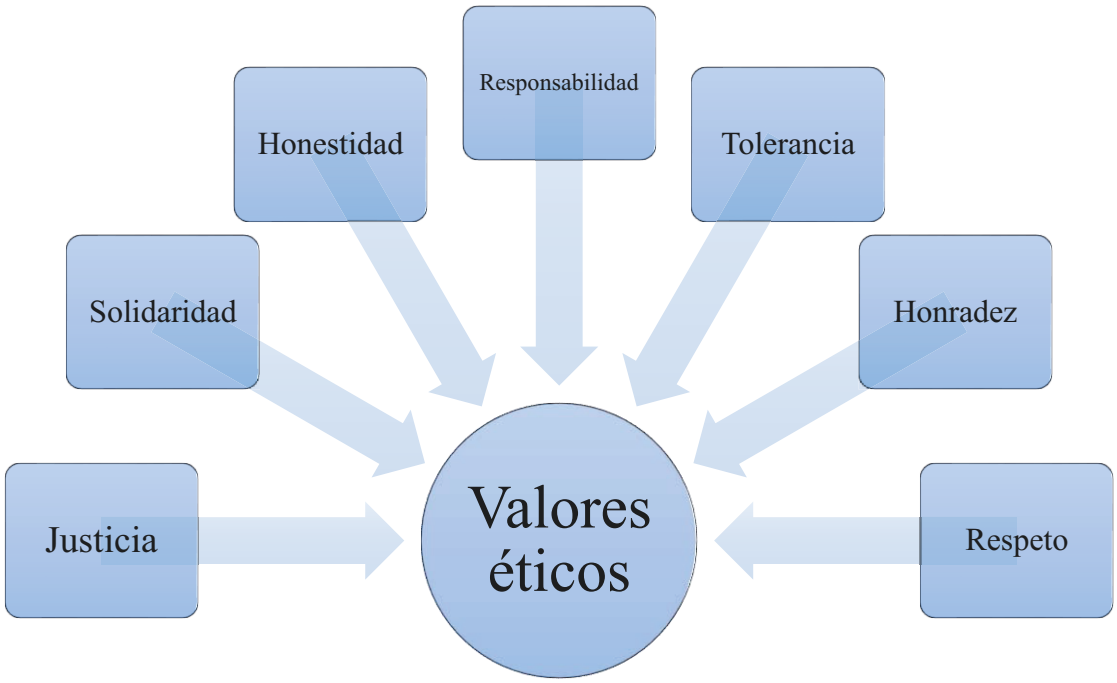


Figura 1 - Valores éticos del auditor

Ámbito de aplicación de auditoría informática

La auditoría informática sirve para detectar evidencias de riesgos y/o problemas en el apoyo informático a los procesos del negocio originados por un mal uso informático y/o del control. Además de esto, la realización de un informe como producto final de la auditoría generará un listado de mejoras y recomendaciones, tanto en infraestructuras como en procesos TI, que se deberán aplicar para mejorar la rentabilidad y eficacia del negocio. Existen tres áreas principales en las cuales se puede realizar una auditoría:

- Seguridad física referida a los dispositivos informáticos del negocio
- Confidencialidad y seguridad de la información
- Legislación y economía

La seguridad física atañe a los elementos de hardware que componen la infraestructura TI del negocio y que han de protegerse frente a agresiones externas, hurtos o mal uso. Otro punto a controlar es el acceso a las oficinas e instalaciones de las oficinas, para prevenir posibles robos tanto de elementos físicos como de información. Otro elemento a controlar son los proveedores. Son necesarios una serie de contratos para estipular los tiempos de respuesta de los proveedores frente a fallos de servicio. Por

ejemplo, una caída de la red de voz y datos ha de solucionarse enseguida, mientras que la rotura de un ratón es menos crítico para el negocio.

Por otra parte se trata de verificar la seguridad lógica frente a ataques informáticos, intrusiones externas, borrado de información mediante aplicaciones y configuraciones de los sistemas de seguridad y comunicaciones (*routers*, cortafuegos). Debido a la importancia que tiene la Información en la empresa, se ha de cuidar la confidencialidad y la seguridad de ésta. La confidencialidad de la información establece que los canales de comunicación han de ser seguros y confiables, de modo que la información enviada sea la misma que se recibe en el destinatario; así como evitar que los datos almacenados puedan ser modificados o alterados, incluso eliminados.

Existen dos tipos de legislaciones que se pueden aplicar a los sistemas TI. Se trata de la L.O.P.D. y la L.S.S.I. de las cuales hablaré más adelante con más detalle. Además de estas leyes, hay que prestar especial atención a los delitos informáticos que podrían englobarse en dos grupos: aquellos que atentan contra el sistema informático y aquellos que se ejecutan por medio del sistema informático. Como en todo negocio, el principal objetivo es la economía, y la auditoría informática también ha de emplearse para comprobar que exista un equilibrio entre los riesgos asumidos, los costes derivados de implantar una determinada seguridad y su eficacia. La eficacia del sistema se puede calcular por la rentabilidad que puede obtener el negocio de los datos almacenados en el sistema, de su veracidad y de la rapidez con la cual son generados. Todo esto ayuda a que la Directiva de la empresa pueda tomar decisiones estratégicas óptimas para el negocio.

Como podemos apreciar en la siguiente figura, existen distintos elementos dentro del negocio que intervienen en el concepto de seguridad.

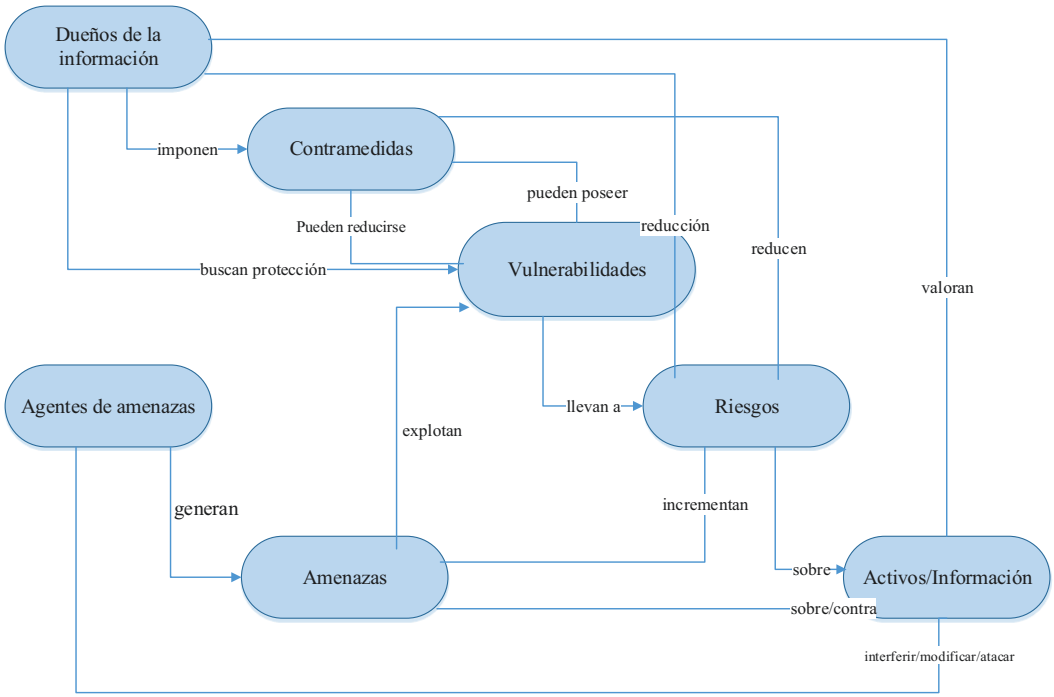


Figura 2 - Conceptos y relaciones de seguridad TI

Tipos de auditoría informática

Según los elementos auditados, pueden existir varios tipos de auditoría informática. En el presente proyecto, se realizará una auditoría completa en la que entren en juego distintos tipos de auditoría [*ai_eche*]:

- Auditoría de la gestión: en este tipo, se analizan las relaciones de la empresa con los proveedores de servicio, así como la contratación de bienes. Los proveedores de servicios pueden ser tanto externos como internos, en el caso del departamento de TI y el resto de la empresa. Por otra parte, se estudia también toda la documentación relacionada con las aplicaciones informáticas.
- Auditoría legal de la normativa regulatoria: estudia que se estén cumpliendo las leyes sobre manipulación y gestión de información sensible de acuerdo a lo estipulado en la Ley Orgánica de Protección de datos, análisis de la Ley de Propiedad Intelectual.

- Auditoría de los datos: se clasifican los datos según su criticidad, se analizan las aplicaciones para verificar su correcto funcionamiento y su seguridad. Y se analizan los flujos internos y externos de información. Los flujos externos de información son las comunicaciones existentes entre personal de la empresa y clientes o proveedores.
- Auditoría de almacenaje de datos: aunque se pueda confundir con la "auditoría de los datos" este tipo de auditoría analiza y verifica la seguridad de los *contenedores* de estos datos. Se encarga de controlar los accesos, gestionar permisos de forma que se pueda asegurar la integridad y calidad de los datos almacenados.

A modo de paréntesis, añado una tabla que muestra la legislación española concerniente a la Información y los Datos.

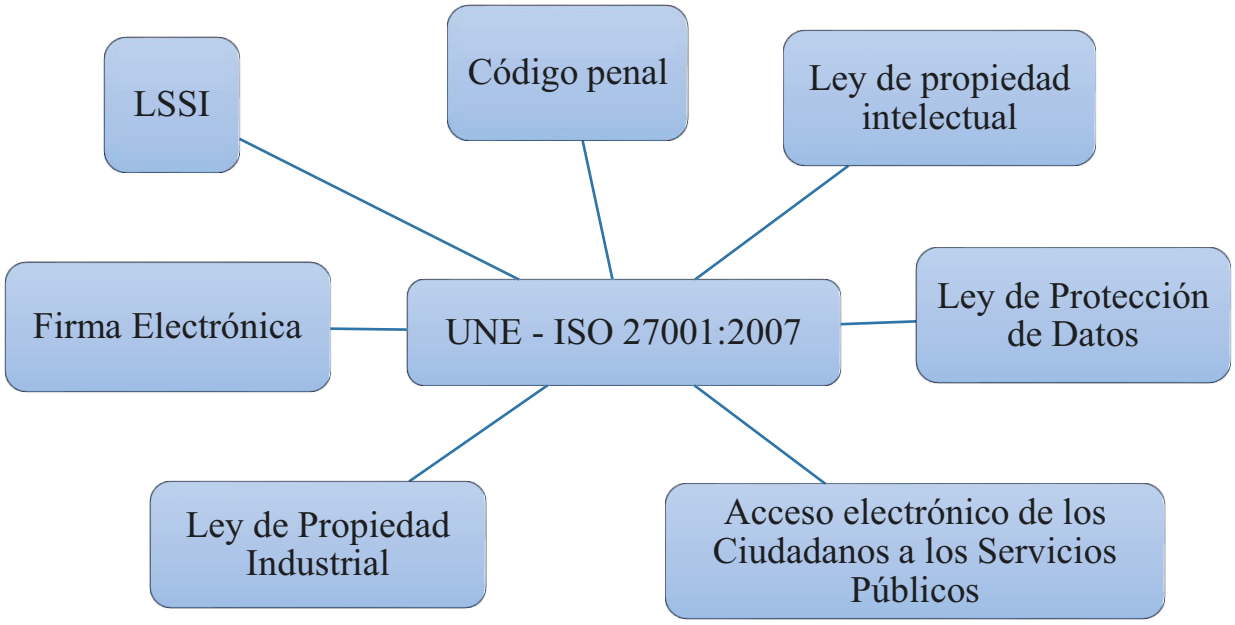


Figura 3 - Legislación española

- Auditoría de la Seguridad Física: esta auditoría se refiere al emplazamiento de la empresa y la seguridad de su infraestructura. Se emplea para evitar posibles situaciones de riesgo, protección de emplazamiento incluso manteniendo en secreto ubicaciones de parte de la infraestructura (servidores espejo y copias de seguridad). Por otra parte, también cubre el control de acceso a las instalaciones de la empresa.

- Auditoría de la Seguridad Lógica: además de la protección de los elementos lógicos por excelencia de la informática: los datos, este tipo de auditoría cubre el control de la autentificación de usuarios. Esta auditoría también estudia los procesos de autentificación y cifrado en los procesos de comunicación. De esta forma también se asegura la integridad de la información transmitida.

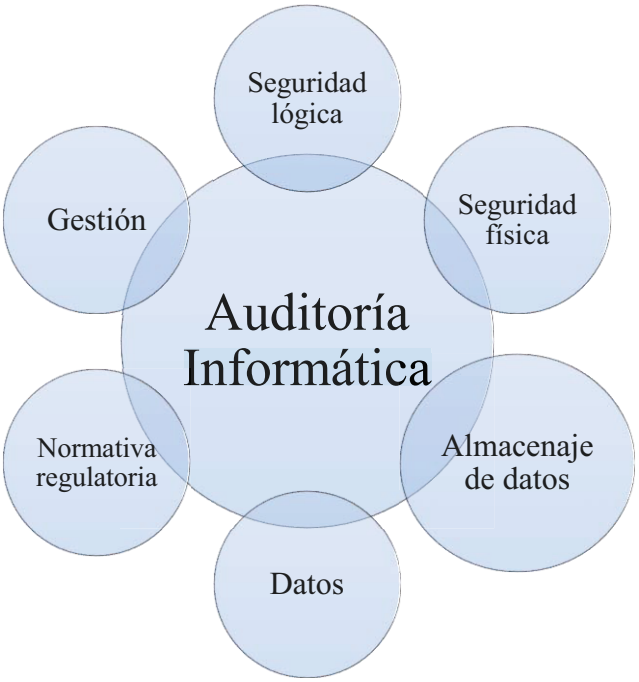


Figura 4 - Tipos de ASI

Como se puede observar, es muy difícil realizar una única auditoría sin invadir el campo de aplicación de otro tipo de auditoría. Es por ello, que para una auditoría informática completa y eficiente, se mezclarán todas estas auditorías en una sola.

¿Qué es CObIT?

CObIT [*cob41*] es el acrónimo de ***C****ontrol* ***OB****jectives for* ***I****nformation and related* ***T****echnology*, a saber, Objetivos de Control para Información y Tecnologías relacionadas. Es el modelo empleado para el Gobierno [*gobti_norm*] de TI dentro de una compañía desarrollado por las organizaciones ISACA

[*isaca*] y el ITGI (*IT Governance Institute*) para llevar a cabo el gobierno de TI en las empresas. Este conjunto de buenas prácticas hace hincapié en el cumplimiento regulador y ayuda a la empresa a aumentar el valor del departamento de TI y elimina el pensamiento general de que dicho departamento es un gasto para la empresa favoreciendo así el alineamiento de TI con el negocio.

Figura 5 – Áreas de enfoque del Gobierno TI

Su misión es la de "*investigar, desarrollar, publicar y promover un conjunto internacional, autorizado y actual de objetivos de control en tecnologías de información generalmente aceptados por el uso cotidiano de gerentes de organizaciones y auditores*". Por lo tanto, la consecución de CObIT es proporcionar una guía estándar que tenga buena aceptación en cualquier empresa de cualquier país sobre los objetivos de control presentes en un ambiente de gestión de Tecnologías de Información para lograr la alineación con los objetivos del Negocio.

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de la Información relacionada. Cada vez más, muchas empresas entienden que la información y la tecnología que la soporta forman parte de sus activos más valiosos, por lo tanto reconocen los beneficios que la tecnología puede proporcionar al negocio. Por otra parte, también reconocen la existencia de riesgos asociados a la implementación y uso de estas nuevas tecnologías. Por ello, CObIT sirve para salvar esa frontera existente entre los riesgos del negocio, las

necesidades de control y los aspectos técnicos y proporciona unas "buenas prácticas". Este conjunto de "buenas prácticas" se emplea para asegurar la calidad, la seguridad, la eficacia y la eficiencia en TI, lo cual es necesario para la alineación de TI con el negocio: identificar riesgos, dar valor al negocio, gestionar recursos y la medición del desempeño. Por recursos, CObIT propone la siguiente clasificación:

- Datos: son los elementos de información con los que trabaja la compañía, tanto información interna como externa.
- Sistemas de Información: aquellas aplicaciones empleadas por la compañía para realizar procedimientos manuales o programados.
- Tecnología: toda la infraestructura TI de la empresas, desde los dispositivos físicos (*hardware*) hasta los sistemas operativos, red de comunicación, etc.
- Instalaciones: recursos necesarios para alojar los sistemas de información de la compañía.
- Recursos humanos: aquí se incluye el personal de la compañía que gestiona los elementos de SI, pero no sólo las personas como tal, sino la habilidad y productividad de éstas para adquirir, planear, prestar soporte y monitorizar los sistemas y servicios de información.

CObIT cubre las cuatro áreas de enfoque del Gobierno de TI del negocio y evalúa la madurez de la empresa mediante objetivos de control pertenecientes a los procesos que forman cada área de negocio de TI. Proporciona una metodología simple genérica y estructurada a alto nivel para auditar los controles de TI sin importar la realidad tecnológica de cada caso.

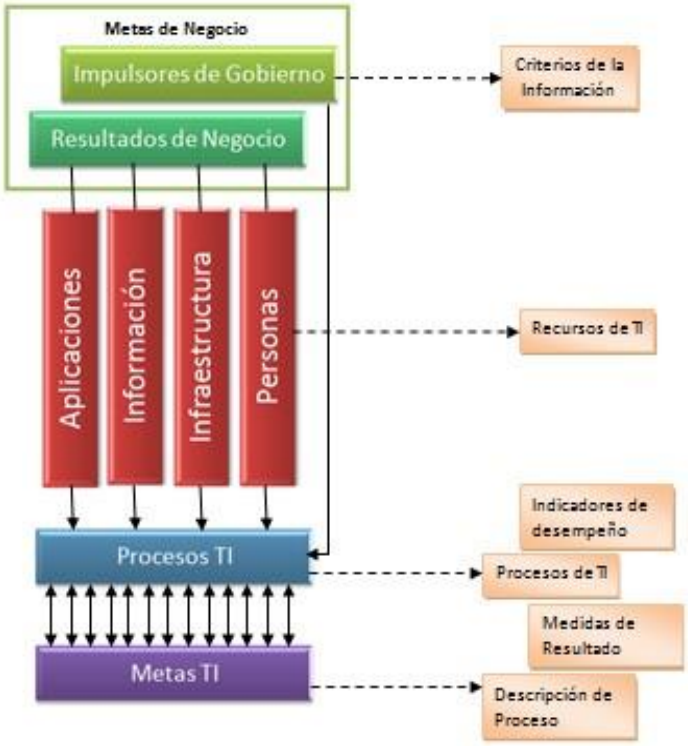


Figura 6 - Estructura de CObIT

Las organizaciones deben perseguir unos estándares de seguridad y calidad tanto para su información como para sus activos. La administración de la empresa debe hacer todo lo posible para lograr el equilibrio en el empleo de los recursos disponibles (personal, instalaciones, tecnologías, aplicaciones y datos) mediante un sistema de control interno. Este sistema de control interno (o marco referencial) ha de ser preciso en la forma en la que cada actividad individual de control cumple con los requerimientos de información y puede repercutir en los recursos de TI. Este impacto se resume en el Marco Referencial de CObIT junto con los requerimientos e información del negocio que han de ser alcanzados (efectividad, eficiencia, confidencialidad, integridad, etc.). Este control está formado por políticas, prácticas y procedimientos organizacionales y su ejecución es responsabilidad de la administración. Por lo tanto, es la administración quien, a través de este Gobierno Corporativo, se encarga de que todos los empleados del negocio cumplan con todos estos objetivos de control. La siguiente figura muestra el cubo de CObIT que ilustra cómo se interrelacionan estos elementos dentro de la compañía.

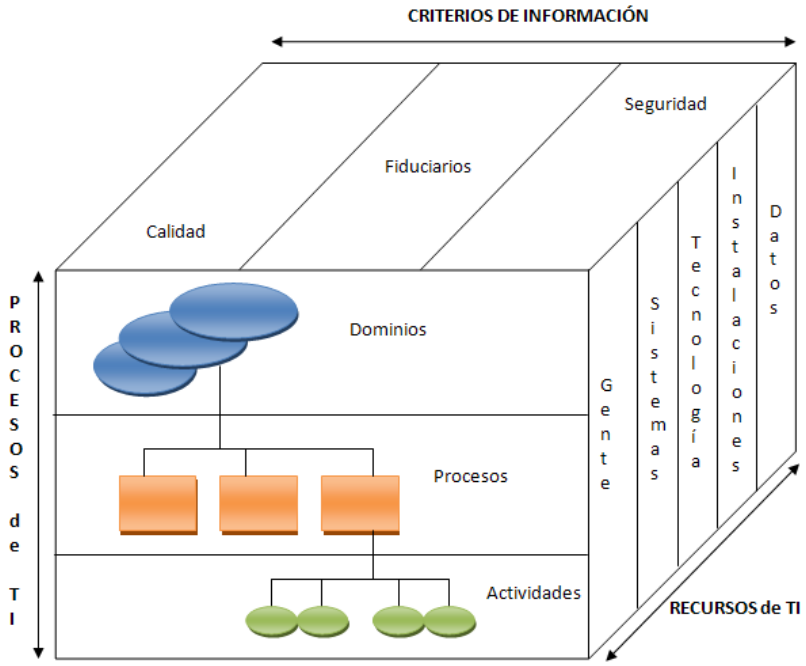


Figura 7 – Cubo de COBIT

.

Los procesos de IT que define COBIT se dividen en tres niveles:

- Dominios: este nivel agrupa los procesos TI en base al área organizacional a la que pertenecen.
- Procesos: se trata de un conjunto de actividades unidas bajo un mismo fin.
- Actividades: son las acciones requeridas para lograr un resultado medible mediante el cumplimiento de los objetivos de control.

Los objetivos de control tienen como principal objetivo la identificación de indicadores de rendimiento de la infraestructura de SI y no se trata de definir un marco de cualificación. COBIT es un fundamento general, no estamos hablando de un conjunto de criterios de evaluación como pueden serlo ITSEC, TCSEC o las evaluaciones de la ISO9000.

Estos elementos se organizan según lo mostrado en la siguiente figura que compone el marco de trabajo completo de CObIT:

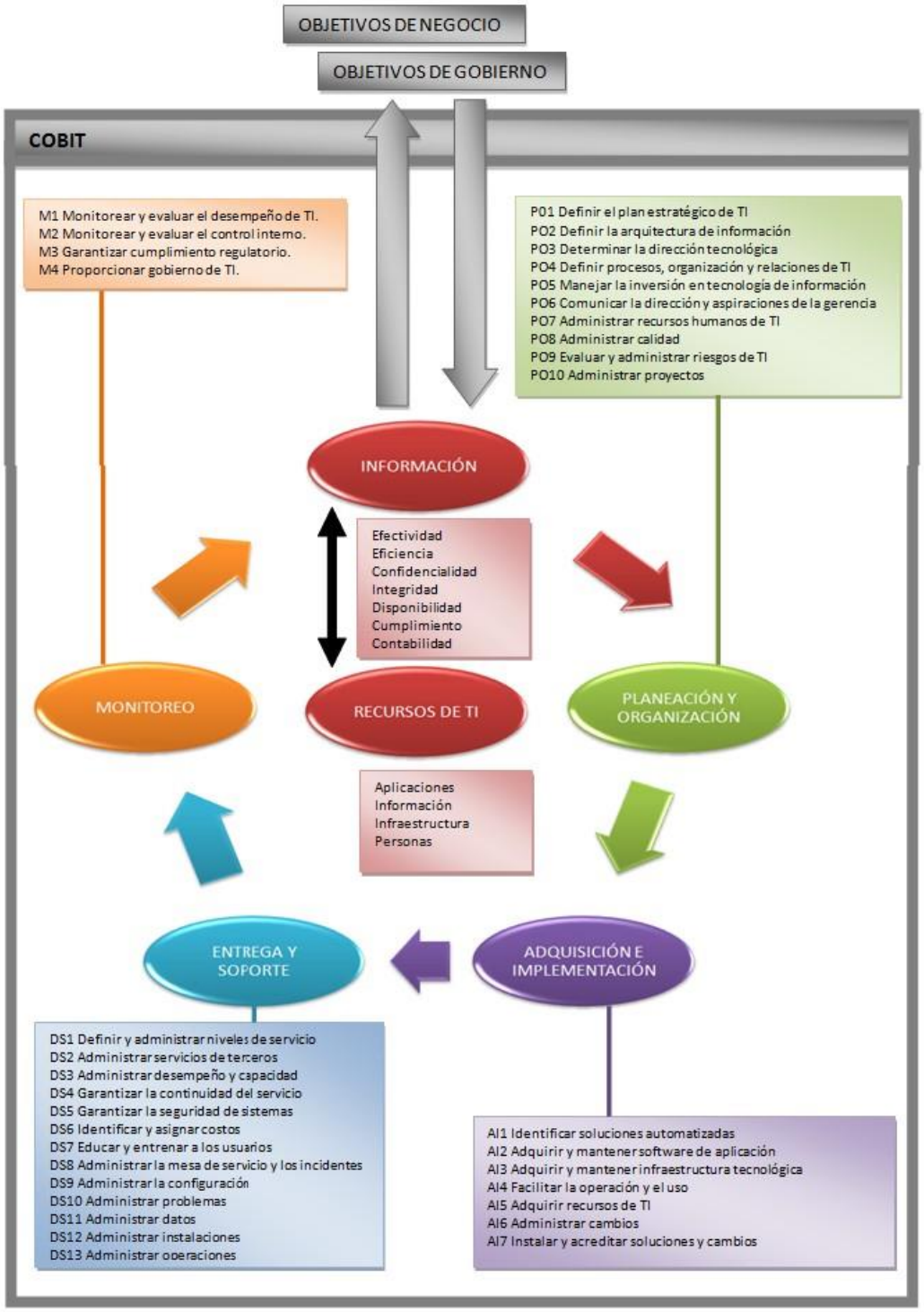


Figura 8 – Marco de trabajo CObIT

Las propiedades que ha de cumplir la información con la que trabaja CObIT son las siguientes:

- Efectividad: la información ha de ser relevante y de utilidad para los procesos del negocio.
- Eficiencia: la información se obtiene mediante el uso más rentable de los recursos disponibles.
- Confidencialidad: asegurar la protección de aquellos datos con contenido sensible.
- Integridad: verificar que el contenido de la información que maneja la compañía no se ha visto alterado sin autorización.
- Disponibilidad: punto relativo a la posibilidad de acceder a la información cuando las necesidades del negocio así lo requieran.
- Cumplimiento: se trata del cumplimiento regulatorio de la información.
- Confiabilidad: hablamos en este caso de proveer la información apropiada para que la administración del negocio pueda gestionar la compañía y cumpla con sus obligaciones de gobierno.

Legislación aplicable

L.O.P.D.

Como hemos visto anteriormente, uno de los objetivos de la ASI, es asegurar el correcto funcionamiento de la infraestructura (lógica y física) de TI, que permite una correcta gestión de la información, lo que permite continuar con el correcto desarrollo del negocio. Cualquier entidad mercantil, sin importar su tamaño, sea cual sea la personalidad jurídica con la cual opere, recaba una serie de información y datos de carácter personal de sus clientes, ya sea en formato papel o, cada vez más, en formato electrónico. Están sometidas al cumplimiento de esta ley con el fin de salvaguardar el derecho a la intimidad de los clientes o de aquellos usuarios que tengan contacto con la compañía. Previa a la vigente Ley Orgánica de Protección de Datos, estuvo vigente la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos (LORTAD) [*lopd*]. A fin de que se cumpla esta normativa, está presente la Agencia Española de Protección de Datos y entre sus principales funciones está la de atender a los afectados, supervisar el tratamiento de datos personales por parte de las empresas, elaborar normas enfocadas a la protección de datos y promover una cultura de protección de los datos personales.

La LOPD tiene por objeto garantizar y proteger en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas. Por otra parte, se encarga de establecer una serie de medidas de seguridad para los ficheros informatizados y los que no lo son que contengan datos de carácter personal. Clasifica estos ficheros en tres niveles de seguridad (alto, medio o básico) en función de la naturaleza de los datos contenidos en estos ficheros.

Por todo ello, es un punto importante para la empresa el buen cumplimiento de la normativa incluida en la LOPD acerca de la protección de datos [*lopd_pyme*]. De lo contrario, se vería afectada por unas penalizaciones que, además de suponer un gasto económico, supondrían un grave perjuicio a la imagen de la empresa y una pérdida de confianza con respecto a sus clientes. Se tendrá que analizar la información que maneja el bufete para determinar los niveles de seguridad de ésta, y seleccionar adecuadamente qué artículos de la LOPD son aplicables y han de cumplirse.

Por otra parte, hay que tener en cuenta que tras la aparición de la *nube* y de los servicios de sincronización (empleados en el bufete para poder trabajar en remoto con datos almacenados en el bufete), cada vez se almacenan más cantidad de datos en esas ubicaciones. Hay que asegurarse de que estas empresas cumplan también la LOPD al operar con una empresa española, sujeta a esta normativa.

Real Decreto 1720/2007, de 21 de Diciembre.

Se trata del reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal [*boe_lopd*]. El Real Decreto es un conjunto de artículos que cumplimentan los artículos [*boe_lopd_rd*] presentados en la Ley Orgánica. Posteriormente, en el ANEXO I, paso a citar todos los artículos que han sido utilizados o nombrados en la realización de esta auditoría.

Por otro lado, establece la obligación para todas las organizaciones (privadas o públicas) de poner en marcha las medidas necesarias de seguridad sobre los sistemas informáticos, locales, soportes de almacenamiento, personal y procedimientos operativos que vayan a estar en contacto con estos datos sensibles.

L.S.S.I.

La Ley 34/2002 de 11 de Julio [*lssi*] se aplica a empresas de comercio electrónico y a otros servicios de internet en el caso de que éstos formen parte de su actividad económica. Esta ley se encarga de regular las obligaciones de los prestadores de servicios y los servicios que prestan. Estrictamente, un

bufete de abogados podría no estar incluir en este grupo de empresas ya que no presta sus servicios por internet ni realiza comercio electrónico. Pero sí que se realiza una toma de contacto previa entre cliente y abogado a través del portal web o de correo electrónico del mismo modo que intercambia información a través de correo electrónico, reportándole así una serie de beneficios económicos y esa operativa sí que se rige por la LSSI.

Para aplicar esta ley, he considerado el bufete como prestatario de servicios Se pueden considerar Servicios de la sociedad de la información: *"Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."*

En el presente caso, el bufete dispone de un blog público en el que emiten diversas opiniones, enlaces a páginas externas que pueden ser objetivo de esta ley así como el groso de su negocio: la comunicación electrónica con sus clientes. En la página web hay información sobre su actividad, productos, formularios de contacto. En este caso, el bufete estaría obligado a facilitar los datos de información general establecidos en el artículo 10. [*lssi_rd*]

La ley comprende un total de 45 artículos divididos en 7 títulos y finaliza con una serie de disposiciones y un anexo que pasaré a enunciar en el Anexo II del mismo modo que he hecho para la LOPD.

Ley de Propiedad Intelectual

El portal web del bufete contiene una sección de noticias y artículos en los cuales dan cabida a multitud de leyes y normativas, así como menciones a varios artículos del Boletín Oficial del Estado. Se trata de una ley aprobada en 1987 y modificada en varias ocasiones hasta la actual en el Real Decreto Legislativo 1/1996, de 12 de Abril, que regula los derechos morales y de explotación [*prop_int*], defendiendo de esta forma los derechos del autor de la obra. Además del principal punto a considerar: ¿quién es el autor? En cuyo caso, el autor sería independiente, siendo este el propio bufete ya que no figura ningún autor en ninguno de sus artículos o noticias.

Otro de los apartados de esta ley son los Derechos Morales y los Derechos de Explotación. Los derechos morales se aplican sobre el autor, que deciden la divulgación de la obra y cómo ha de hacerse.

Del mismo modo, garantiza el respeto a la integridad de la obra y que pueda ser modificada o incluso retirada de la circulación.

Los derechos de Explotación son cuatro:

- Derecho de reproducción, que garantiza que la obra o parte de ella pueda ser reproducida por cualquier medio o forma.
- Derecho de distribución, que se refiere a la disponibilidad pública de la obra, se aplica sobre la puesta de la obra a disposición del público.
- Derecho de comunicación pública, en relación a los actos mediante los cuales la obra es presentada al público.
- Derecho de transformación que permite modificar una obra existente para dar lugar a una nueva.

Por lo comentado anteriormente acerca de los artículos de prensa, así como de reproducción de leyes en el portal web, se podrían aplicar varios derechos de la Ley de Propiedad Intelectual. Obviamente, el Derecho Moral es el principal, ya que la mayoría de escritos que hay en el portal son creación de los abogados del bufete. Sin embargo, en algunos casos, se citan y mencionan algunas leyes y artículos. Y en este caso se tendría que hacer referencia a los derechos de Explotación que he mencionado anteriormente.

3.- Análisis de la situación

Estructura del proyecto

Este proyecto se basa en la realización de una hoja de ruta que sirva de guía para la realización de una auditoría informática, por lo que se va a realizar un análisis de los objetivos de control de COBIT que considero que pueden ser aplicables a la hora de realizar una ASI de un bufete.

Para la realización de la ASI, se han de realizar varios pasos:

- Dimensionar el sistema o la empresa a auditar
- Definir el alcance de la auditoría
- Determinar los recursos disponibles así como el tiempo necesario en la realización de la audición.
- Recopilar y revisar documentación adicional o previa, productos de anteriores auditorías.
- Estimar el coste del proceso.

El dimensionamiento de la empresa consiste en el análisis del negocio y de los datos presentes en él. Esa información puede obtenerse siguiendo los siguientes puntos:

- Generación de documentación básica:
    - Organización del departamento de proceso de datos y líneas de dependencia dentro de la organización.
    - Descripción de la organización.
    - Descripción de los sistemas presentes y de su uso.
    - Información sobre el uso de centros externos a la empresa.
- Obtener información sobre procedimientos, normativas y políticas de la empresa. Esto se puede realizar mediante varias técnicas:
    - Realización de cuestionarios a los empleados: estas entrevistas pueden servir al auditor para contrastar que los usuarios realizan las tareas tal y como vienen especificadas en los correspondientes planes de TI. Pero hay que prestar atención a que estas preguntas y respuestas sean personales y confidenciales durante el proceso de la auditoría. Tanto el auditor debe velar por mantener estos datos seguros, como los encuestados no desvelar el contenido de las entrevistas con otros compañeros de la empresa.

- Observación: tanto de los propios datos de la compañía, como de la forma de trabajar de los usuarios, se pueden desvelar fallos en el manejo de datos e infraestructura TI y malas prácticas de los usuarios. Esta operación ha de realizarse sin interferir en el correcto desarrollo de las operaciones dentro de la empresa y que el uso de los recursos impacte lo menos posible.

Y como punto final de la auditoría, se suele presentar una lista de recomendaciones y planes de acción, que junto con la enumeración de los puntos débiles y amenazas existentes, forman el objetivo final de la auditoría que se le presenta a la Dirección para que tome las medidas oportunas.

Este proyecto se compone del análisis previo del negocio, de forma que se puedan determinar qué procesos de CObIT son necesarios para lograr una correcta alineación de las TIC en la empresa. Y a continuación, se realizará un estudio práctico de estos procesos, aplicándolos sobre un bufete real que sirva como ejemplo para este desarrollo. El resultado de esta aplicación práctica, sienta las bases para que un futuro auditor o grupo auditor pueda realizar, siguiendo los pasos marcados por este proyecto, una auditoría informática de un bufete.

TI en un bufete

No solo en el mundo de la abogacía, sino en muchos otros sectores, la informática está cada vez más presente en el negocio y participa de forma activa en la consecución de objetivos. El principal uso que se le da a las TI en un bufete de abogados es la gestión documental y las comunicaciones, además del tratamiento de información. Hay muy pocos procesos automatizados de TI en un bufete si entendemos como "proceso automatizado" aquel que realiza una máquina con una determinada frecuencia, sin la intervención de un operario. Como ejemplo, están las copias de seguridad que se hacen de la información almacenada en el servidor.

El resto de procesos de TI que se realizan en el bufete, son operaciones iniciadas y llevadas a cabo por personal humano. En algunos casos son operaciones automáticas que se realizan siempre tras haberse iniciado una operación previa (por ejemplo, la clasificación de un CV tras la operación de haberlo recibido vía web) y en otras ocasiones, puede tratarse de operaciones puntuales, como la reposición de un elemento de hardware.

Razones para una auditoría informática

Como ya mencioné anteriormente, los motivos por los que se lleva a cabo una auditoría informática son la revisión y verificación de los procesos de TI, así como de sus recursos y activos. Tan importante es la confidencialidad y seguridad de los datos con los que los usuarios trabajan, toman sus decisiones y se comunican con los clientes; como lo es la integridad y seguridad de la infraestructura TI sobre la que se apoya todo el Negocio. Todo ello se hace con el fin de lograr la alineación de TI con el negocio.

Un proceso de auditoría (ya sea informática o de cualquier otro tipo) puede ser realizado por un equipo externo a la empresa auditada (en caso de que sea solicitada por una empresa externa) o por un equipo interno de la compañía (en caso de que sea una decisión propia de la dirección de negocio) para determinar de qué forma puede mejorar el uso del soporte TI para mejorar su rendimiento y desempeño frente a la clientela. Del mismo modo que logra diferenciarse de la competencia mediante uso más eficiente de las TI. Otra razón puede ser la detección de deficiencias o errores en el negocio provocada por el Dpto. TI.

Sin embargo, aunque la realización de una auditoría no conlleve fallos o problemas previos, en este caso sí que existen una serie de deficiencias en los procesos que podrían eliminarse, así como una falta de ética y legalidad en el empleo de aplicaciones y herramientas de TI.

CObIT

Tal y como expuse en la introducción al hablar de CObIT, se trata en este caso de alinear dos mundos que pueden parecer diametralmente opuestos: TI y el mundo del derecho, para lograr una mejora en la consecución de los objetivos de la empresa. El factor humano en los procesos TI de un bufete es bastante alto, lo cual puede inferir en errores *humanos*. Lo que busco al aplicar CObIT en estos procesos es, en cierto modo, automatizarlos, crear una serie de pautas a seguir en las cuales haya un menor margen de error. Elegí CObIT por encima de otros modelos de buenas prácticas como pueden ser ITIL, CMMI, COSO, MAGERIT, SAC o SAS entre otras [*gobTI_ieee*] porque me parecía una buena política de buenas prácticas de TI para implantar en una empresa como un bufete, un tipo de empresa con un moderado uso de las TI y cuya finalidad del negocio no es el desarrollo de servicios TI. Se trata de una entidad en donde las TI no son estratégica o absolutamente críticas para la supervivencia del negocio. No estamos hablando de una consultora tecnológica o una factoría de Software, sino de una compañía

que por la naturaleza de su negocio y la formación de sus empleados, puede ver las TIC como algo ajeno a ellos.

Como ya he explicado anteriormente, CObIT es un conjunto moderno y estándar de objetivos de control de las TI. Moderno ya que está en constante actualización y revisión por parte de los miembros de varios países de la ISACA/F de cara a mantener estos objetivos de control actualizados y coherentes con los actuales SI existentes en las empresas. Y estándar ya que es pragmático y válido para las necesidades de gestión, al mismo tiempo que puede ser utilizado sin importar el tipo de TI que la empresa tenga implantadas y en cualquier compañía. CObIT forma un conjunto de objetivos de control interesante ya que gracias a estas características, se puede aplicar en el amplio espectro de los SI de la empresa.

Como ejemplo de la organización jerárquica de CObIT, a continuación un ejemplo con uno de los procesos del dominio "Entregar y dar soporte" (DS):

- Dominio: Entregar y dar soporte (DS)

  - Proceso: Administrar los Servicios de Terceros (DS2)

    - Actividad: Gestión de Relaciones con proveedores (DS2.2)

      Para asegurar que esta actividad se cumple correctamente, se establece como objetivo de control la existencia de un contrato con este proveedor.

Como indica la guía de CObIT, estas actividades no son obligatorias, por la naturaleza de cada empresa, pueden no estar presentes, por lo tanto mi guía CObIT no presenta todas las actividades y controles presentes en la guía. El motivo de haber elegido CObIT como metodología es que satisface ampliamente las necesidades que tiene la compañía en relación al uso de TI, teniendo en cuenta los requerimientos de la empresa, organizando sus actividades mediante el modelo de procesos, identificando los recursos TI y definiendo los controles de éstos.

I - Planear y organizar

1.- Definir un plan estratégico de TI – PO1

La definición de un plan estratégico de TI se hace necesaria para administrar y dirigir todos los recursos de TI de acuerdo con la estrategia del negocio. Este plan estratégico tiene por objetivo mejorar el entendimiento de los involucrados al respecto de las limitaciones y posibilidades de TI, evaluar el rendimiento actual y determinar las necesidades de inversión. Este plan estratégico desemboca en un plan táctico.

Objetivos de control:

- Existencia de un plan de Sistemas: se trata de un plan interno de sistemas en el que se han de plasmar las acciones a tomar en lo referente a TI dentro de la empresa
- Coherencia del plan de sistemas: este plan de sistemas ha de proyectar acciones coherentes con la actividad del negocio y la estructura de la empresa.
- Confirmación por parte de los implicados: se han de reunir los responsables de los diversos departamentos implicados y relacionados con las operaciones de TI para dar el visto bueno a dicho plan, asegurando el entendimiento de las capacidades actuales de TI.

Obj. Control	Descripción
Existencia de plan de sistemas	Se trata de un plan interno de sistemas, en el que se han de plasmar las acciones a tomar en lo referente a la gestión de TI dentro de la empresa
Coherencia del plan de sistemas	La finalidad del plan es la proyección de acciones de SI cuyos resultados sean coherentes con la actividad del negocio y la estructura y dimensión de la empresa.
Acuerdo entre implicados	A fin de validar este plan de sistemas, todos los implicados se tienen que reunir para validarlo y realizar modificaciones en caso de que no haya acuerdo por ambas partes

Tabla 1- Proceso PO1

2.- Definir la arquitectura de información – PO2

Este objetivo se centra en el tipo de datos que maneja el negocio para sus actividades así como el soporte físico en el cual se almacena.

Objetivos de control:

- Incluir el apartado de Almacenamiento de Información en el plan de TI.
- Definir el tipo de soporte físico en el que se almacenará la información.
- Organizar los archivos con los que se trabaja en el negocio según tipos (documentos, PDF's resultantes de escaneos, correos electrónicos) y establecer máscaras de nombre para los distintos tipos de ficheros. Estas máscaras de nombrado ayudarán a determinar el origen del fichero y su fecha, algo de importancia en el negocio de un bufete.
- Clasificación de documentos: existirán datos sensibles con información privada, datos externos recibidos de clientes, datos de comunicación interna.

Obj. Control	Descripción
Incluir sección de Almacenamiento de datos en Plan TI	El plan de gestión de los SI acordado en el punto anterior ha de incluir una sección referida al manejo y mantenimiento de datos.
Tipo de soporte físico de almacenamiento	Determinar en qué soportes físicos se almacenará la información.
Organización documental	El bufete trabaja con distintos tipos de documentos según el uso que le den. Han de estar correctamente identificados para un rápido acceso a ellos, con una normalización establecida para el nombrado de los distintos ficheros existentes en el bufete.
Clasificación documental	Los ficheros manejados en el bufete se organizan según la sensibilidad de los datos que contienen. Mediante las clasificaciones que proporciona la LOPD de los tipos de datos sensibles, se establecen los distintos niveles de seguridad de los datos.

Tabla 2 - Proceso PO2

3.- Administrar la Inversión en TI – PO5

La dirección del negocio ha de ser consciente de la importancia que tiene el departamento de TI dentro de los buenos resultados de la compañía. Por ello se ha de administrar correctamente la inversión en el grupo de Gestión de TI de la empresa. Una falta de previsión económica podría acarrear graves consecuencias en el correcto cumplimiento del negocio de la empresa. Se definen los siguientes objetivos de control:

- Determinar la existencia de un plan estratégico de costes: formando parte del plan de GSI definido dentro del plan estratégico de la empresa, se encuentra definido el plan de costes de TI dentro del cual se indicará la partida presupuestaria de dicho departamento, así como los encargados de la gestión del mismo.
- Inventariado de equipos: este punto de control analiza que se estén adquiriendo los equipos según las necesidades de los usuarios y no sean dispositivos con características sobredimensionadas. Por otra parte, se vigila que exista una malversación de fondos de la partida del Dpto. TI realizando un análisis comparativo de los gastos y el inventario existente.
- Procesos de renovación o reparación de equipos de la compañía: a la hora de renovar o arreglar un dispositivo habrá que analizar factores como la necesidad real por parte de los usuarios, la relación entre el coste de renovación frente a la reparación del dispositivo y el rendimiento que se puede obtener de un dispositivo reparado frente a una nueva adquisición.

Obj. Control	Descripción
Plan estratégico de presupuestos de la compañía	Dentro del plan de sistemas establecidos en el punto "PO1" se incluye este apartado de presupuesto para el dpto. de SI.
Inventariado de elementos	Un inventariado incorrecto puede derivar en problemas de aprovisionamiento de material necesario para la continuidad del negocio.
Reparación/renovación de equipos-software	Para determinar en qué momento ha de sustituirse un elemento o renovarlo.

Tabla 3 - Proceso PO5

4.- Administrar los recursos humanos de TI – PO7

Pese a que el principal elemento del Dpto. TI es la información y los dispositivos, son las personas quienes gestionan, administran y mantienen estos elementos. Este proceso de dominio sirve para administrar y gestionar el personal del Dpto. TI. Y abarca los campos de reclutamiento, formación, evaluación de personal y promoción profesional.

Objetivos de control:

- Contratación de personal de TI: para este apartado no se puede definir un plan con fechas y plazos, ya que la contratación de personal depende del estado actual de la plantilla de TI, aunque se podría tratar de analizar una serie de métricas que podrían determinar un cierto ciclo de vida en la contratación de nuevo personal para tratar de hacer una previsión en este proceso. Sin embargo, se puede establecer un proceso de búsqueda de personal: contacto con el dpto. de RRHH, altas en páginas web de contratación de personal.
- Estructurar el proceso de búsqueda de personal: contactar con el dpto. de RRHH, establecer un canal de recepción de CV (alta en páginas web de contratación, sección en página web corporativa)
- Formación del departamento de RRHH: es necesario aleccionar al personal de RRHH sobre los conceptos y nociones necesarias para ser contratado en el Dpto. TI.
- Definición del proceso de selección: esto consiste en asignar personal de RRHH competente para realizar las entrevistas, en clasificar y almacenar correctamente los CV's y en procesar los resultados obtenidos de las reuniones con candidatos.
- Plan de formación TI: tiene que existir un plan de formación continua para los empleados de TI. De esta forma se consigue una mayor competencia y motivación y se evita que el conocimiento se centre en una sola persona.
- Plan de evaluación: definir una periodicidad con la cual se evaluarán los conocimientos y competencias de los empleados de TI. De este modo también se controlará si el plan de formación es correcto o necesita renovarse.
- Gestión de la dependencia de personal TI: Para hacer frente a un despido no planeado o un cese de algún miembro del personal de TI, se hace necesaria la documentación de los conocimientos y procedimientos que ejecuta cada uno de los miembros del Dpto. TI. De esta forma se evitan dos posibles problemas: que el conocimiento se concentre en una única persona y que, en el

caso de un cese temporal (vacaciones, periodo sabático), otra persona sea capaz de sustituirla y realizar sus tareas.

Investigación del personal: debido al carácter sensible de la mayor parte de la documentación que se trata en un bufete, creo que es muy recomendable que este proceso se verifique en un bufete. Se trata, evidentemente, de requerir antecedentes del personal contratado.

Obj. Control	Descripción
Búsqueda de candidatos para TI	Establecer los canales de búsqueda, páginas web, canal de recepción de CV y gestión de los mismos.
Contratación de personal de TI	Analizar el proceso por el cual se realizan las contrataciones de personal para TI.
Formación del dpto. de RRHH	Formación de TI para el personal del dpto. de RRHH.
Definición del proceso de selección	Asignar personal competente para las entrevistas, definir el contenido de las entrevistas (preguntas técnicas, pruebas)
Plan de formación continua TI	Compuesto por cursos (externos e internos) además de la propia formación recibida por el personal de la empresa.
Plan de evaluación de competencias	Análisis de los conocimientos del personal de TI, así como de su uso en sus labores cotidianas.
Gestión dependencia de personal TI	Documentar la información y tareas que realiza cada empleado del Dpto. TI.
Antecedentes del personal TI	Realizar la comprobación de antecedentes al contratar personal TI dada la naturaleza de los datos que se manejan en un bufete.

Tabla 4 - Proceso PO7

5.- Evaluar y administrar los riesgos de TI – PO9

La finalidad de este objetivo de control es plantear un marco de trabajo en el que se puedan administrar los riesgos de TI que puedan afectar a la correcta consecución del negocio. Se identificarán estos riesgos, se evaluarán, se calculará el coste de asimilarlos y se comunicarán estos resultados a la gerencia.

Se presenta el concepto de "evento", que es una amenaza a tener en cuenta que puede explotar alguna vulnerabilidad del negocio considerable, que puede tener repercusiones económicas.

Los puntos de control a revisar son los siguientes:

- Integración en marco de trabajo de riesgos de la compañía: todos los departamentos de negocio conllevan riesgos, y como parte importante de la empresa, todos los riesgos derivados del Dpto. TI han de poder ser administrados correctamente.
- Identificar eventos: evaluar el entorno del negocio para determinar los posibles eventos que puedan repercutir negativamente en la operativa del negocio. Estas repercusiones pueden ser de cualquier ámbito, económico, regulatorio, social, humano, etc.
- Administración de los riesgos: calcular la probabilidad de que sucedan estos eventos y el impacto de sus riesgos en el negocio. Desarrollar un plan de respuesta a estos riegos para anular o minimizar las consecuencias en la empresa y establecer unas medidas para mantener y actualizar este plan.

Obj. Control	Descripción
Definir plan de riesgos de TI	Incluir el plan de riesgos de TI en el marco de trabajo de riesgos de la compañía.
Identificar eventos de riesgo para la compañía	Reconocer los posibles eventos relacionados con TI que puedan causar perjuicios al negocio para su tratamiento.
Administración de riesgos TI	Tras la identificación de los riesgos, trazar un plan para su prevención o resolución.

Tabla 5 - Proceso PO9

6.- Administrar proyectos – PO10

Este proceso tiene como propósito la correcta gestión y administración de proyectos de TI establecidos dentro del marco de un bufete. En este caso, los posibles proyectos serían el desarrollo y mantenimiento de la web corporativa y los aplicativos para la gestión interna de datos. Por otra parte, otros proyectos

más enfocados al hardware y software son las copias de seguridad y dispositivos físicos para los usuarios. Puede ocurrir que varios proyectos estén en marcha en el mismo plazo de tiempo, por lo que es necesario establecer un plan que determine las prioridades.

Objetivos de control:

- Creación de portafolio de proyectos TI: en él se incluirán desde los proyectos estratégicos (posicionamiento de la web) hasta proyectos tácticos como la gestión de infraestructura informática.
- Priorizar recursos: puesto que varios proyectos pueden ser concurrentes en el tiempo, se debe de establecer las prioridades en el empleo de los recursos TI.
- Asignación de presupuestos: el coste del desarrollo de estos proyectos tiene un presupuesto que ha de ser aprobado por la gerencia del negocio.
- Creación de protocolos para el desarrollo y mantenimiento de los proyectos: definir un ciclo de vida apto para los proyectos.

Obj. Control	Descripción
Portfolio de proyectos TI	Analizar la existencia de un portfolio de proyectos TI de la empresa.
Priorizar los recursos TI	Se establecen prioridades en el uso de los recursos TI a la hora de desarrollar e implantar los proyectos.
Asignación de costes a proyectos TI	Asignar costes a los proyectos en función de su tiempo de ejecución, personal involucrado, recursos.
Gestión de ciclo de vida de proyectos TI	Se definen una serie de procesos para el desarrollo y mantenimiento de los proyectos de TI desarrollados para la continuación del negocio.

Tabla 6 - Proceso PO10

II - Adquisición e implementación

1.- Identificar soluciones automatizadas – AI1

Algunos procesos de gestión de SI de la empresa no requieren de la intervención de usuarios de TI, son operaciones o procesos que se realizan de forma periódica.

- Identificar procesos: Analizar y estudiar los procesos que se realizan en el negocio para determinar si cabe la posibilidad de automatizarlos.
- Análisis de riesgos: calcular los riesgos derivados de esta tarea, así como aquellos asociados al diseño de la solución automatizada. Se realiza un balance de los dos para determinar si es rentable automatizar la tarea de negocio.
- Análisis de costes: se realiza un análisis del coste de implementar y desarrollar la aplicación TI para soportar la tarea de negocio frente al coste que supone la gestión manual.

Obj. Control	Descripción
Identificar y analizar los procesos de gestión de datos de la empres	Se realiza un estudio de la gestión de datos que realizar la compañía para determinar su periodicidad.
Análisis de riesgos	Identificar los riesgos asociados a la automatización de dicha tarea.
Análisis de costes	Análisis comparativo entre el coste de automatizar la tarea frente al coste de su manejo por un usuario

Tabla 7 - Proceso AI1

2.- Adquirir y mantener software aplicativo – AI2

Siguiendo las necesidades del negocio, el Dpto. TI ha de ser capaz de diseñar o adquirir (según sea el caso en función del coste de desarrollo) el software aplicativo que mejor se adapte a las necesidades o al objetivo estratégico del momento. Tras este proceso, se ha de implantar y mantener en correcto funcionamiento. Los siguientes objetivos de control sirven para este propósito.

Objetivos de control:

- Establecer un marco de reuniones periódicas entre TI y el negocio: gracias a este tipo de reuniones, los responsables de TI conocerán las necesidades (puntuales y continuas) para analizar las posibles soluciones.
- Analizar el mercado y la oferta de aplicativos existente: se realiza un estudio de la oferta del mercado para dar soporte a esta necesidad a fin de presentar las distintas opciones a la Gerencia.
- Evaluar el coste del desarrollo del aplicativo: junto al anterior objetivo de control, se determina si es necesaria la compra o la modificación de un aplicativo ya existente o la creación de uno completamente nuevo, teniendo en cuenta los factores económicos y de riesgo.
- Toma de requisitos con los usuarios: cuando se defina una aplicación en concreto, serán necesarias entrevistas para recopilar información sobre las necesidades del funcionamiento del aplicativo.
- Integración del aplicativo: tras la compra, modificación o desarrollo del aplicativo, llega la fase de integración en el negocio.

Obj. Control	Descripción
Definir un marco de reuniones entre Negocio y TI	Estas reuniones acordadas entre miembros de Negocio y de Dpto. TI permiten a ambos conocer las necesidades de negocio.
Análisis del mercado y oferta existente de productos TI	De cara a satisfacer las necesidades de Negocio, es necesario conocer la oferta de SW y HW.
Evaluar el coste del desarrollo de SW	En conjunción con el anterior objetivo de control, se determinará la necesidad de comprar o desarrollar nuevo software.
Toma de requisitos	Entrevista con el usuario para recoger sus necesidades y transformación de éstas a bajo nivel para la creación del SW pertinente.

Tabla 8 - Proceso AI2

3.- Adquirir y mantener infraestructura tecnológica – AI3

Los proyectos destinados a la adquisición y mantenimiento de infraestructura tecnológica no necesitan de una aceptación y preparación tan profunda como en el caso de los aplicativos. Es necesario establecer un marco de trabajo en el que intervenga la gerencia del negocio, el departamento de administración

y el propio Dpto. TI para tomar esas decisiones. No hay que dejar de supervisar este proyecto por la importancia que tiene para el negocio poder contar con el soporte que presta toda la infraestructura informática: copias de seguridad, ordenadores, pantallas, comunicaciones, etc. El proceso de la compra, implantación y mantenimiento de la infraestructura tecnológica son necesarios para la continuación del negocio

Como objetivos de control para lograr cumplir este punto:

- Crear un plan de compra de infraestructura TI: un plan que tenga en consideración las necesidades actuales y futuras del negocio, así como una imagen de la situación presente de la infraestructura tecnológica de la empresa. Se tendrán en cuenta las repercusiones que tenga la adquisición de nuevos dispositivos en el aleccionamiento de los usuarios, la transición, los riesgos tecnológicos.
- Establecer canal de comunicación: para aquellos empleados que tengan una necesidad o incidencia en lo relacionado con la infraestructura tecnológica.
- Establecer niveles de protección: para mantener la disponibilidad tanto de datos como de elementos físicos de TI se han de establecer unos niveles de seguridad que protejan los elementos de dicha infraestructura, que da soporte a los servicios del negocio.

Obj. Control	Descripción
Plan de adquisición de dispositivos de infraestructura TI	Planear la compra y el mantenimiento de infraestructura TI teniendo en cuenta las consecuencias que puedan derivar en la usabilidad de los usuarios, la gestión de riesgos.
Establecer canales de comunicación	Determinar la forma y canal de comunicación por el cual los usuarios pueden solicitar reparación/renovación de herramientas TI
Establecer niveles de seguridad	Dentro de la gestión de infraestructuras hay que tener en cuenta la seguridad. Tanto el acceso físico como lógico.

Tabla 9 - Proceso AI3

4.- Facilitar la operación y el uso – AI4

El objetivo de este proceso es lograr que tanto el Dpto. TI como los usuarios tengan a su disposición el material necesario para realizar un buen uso de las herramientas TI que están a su alcance. Se trata de un proceso que busca mejorar la operatividad de los usuarios de TI y redundar en mayores beneficios para la empresa. Ya sean mediante unos productos de mayor calidad o por un mayor aprovechamiento del tiempo de trabajo de los empleados. Por todo ello es necesario desarrollar y generar información de empleo a todos los usuarios, tanto de negocio como de TI. Este proceso está cubierto por los siguientes objetivos de control:

- Como principal objetivo de control está la definición de un marco de enseñanza sobre el manejo tanto de herramientas físicas como lógicas de TI (acceso a portal web del usuario, uso de aplicaciones informáticas, manejo de los dispositivos físicos, etc.).
- Transferir conocimiento a usuarios finales: entendiendo estos usuarios como el personal externo al Dpto. TI que ha de hacer uso de herramientas de SI. Estos usuarios finales recibirán la información de cómo manejar aquellas aplicaciones que vayan a utilizar.
- Transferencia de conocimiento a nuevas incorporaciones al Dpto. TI: a la hora de contratar nuevo personal en el Dpto. TI, habrá que transferirles los conocimientos necesarios para mantener y administrar los SI.

Obj. Control	Descripción
Definir marco de conocimiento dentro de la compañía	Definir un plan para determinar qué conocimientos han de transmitirse a según qué personal.
Transferir conocimientos a usuarios de TI	Informar a las nuevas incorporaciones del Dpto. TI el funcionamiento de aplicaciones y los procesos.
Transferir conocimientos a usuarios finales	Según el puesto de trabajo del usuario final, se le transmitirán los conocimientos necesarios.

Tabla 10 - Proceso AI4

5.- Adquirir recursos de TI – AI5

Este proceso gestiona la relación que ha de existir entre la compañía y todas aquellas empresas externas proveedores de servicios de TIC necesarios. En este proceso, el término "recurso de TI" está más enfocado al concepto de prestación de servicios TIC (entendiendo este elemento como uno de los recursos TI de COBIT) que a la adquisición y mantenimiento de infraestructura TI como periféricos, ordenadores, etc que se trata en el proceso AI3.

- Definición del plan de acción para la adquisición de recursos de TI: La dirección de la compañía y el Dpto. TI se encargan de desarrollar y gestionar una política de adquisición de elementos de TI necesarios para la continuidad del negocio.
- Seleccionar proveedores de forma arbitraria y comparativa: seleccionar una serie de proveedores para las distintas áreas de negocio que necesiten elementos TI.
- Establecer los acuerdos y contratos con los proveedores tanto de productos hardware como software para asegurar el correcto mantenimiento y recuperación.
- Gestión de contratos con proveedores de servicios: analizar si el suministro de productos TI corresponde con las necesidades de negocio y los acuerdos que se firmaron al iniciar la relación contractual.
- Adquisición de elementos hardware: realizar la compra de elementos y dispositivos HW en función de las necesidades y del inventario existente.

Obj. Control	Descripción
Plan de acción para adquisición de recursos TI	Definir un plan para la adquisición de elementos TI para el negocio.
Selección de proveedores	Selección de proveedores de servicios TI para el negocio
Gestión de contratos y servicios con proveedores	Gestionar los contratos con los proveedores de servicios para su modificación, anulación, renovación.
Adquisición de elementos de hardware	Gestionar la compra de hardware necesario para el negocio

Tabla 11 - Proceso AI5

III - Entregar y dar soporte

1.- Definir y administrar niveles de servicio – DS1

Definir y gestionar niveles de servicio entre TI y los usuarios del negocio, así como determinar quienes son los responsables y evaluar el funcionamiento del soporte. Este punto es crítico para no perder tiempo a la hora de solicitar apoyo y que la respuesta sea lo más rápida y eficiente posible.

- Definir un portfolio de servicios ofrecidos por el Dpto. TI que será acordado previamente mediante reuniones y puestas en común entre la Dirección y el Dpto. TI teniendo en cuenta las necesidades del negocio. Para la definición de estos servicios, hay que tener siempre presente la orientación del Negocio para que TI vaya siempre en apoyo de Negocio.
- Gestión de los niveles de servicio (SLA): definir los roles y responsabilidades del personal de TI para la respuesta al usuario ante incidencias. Por medio de la definición de estos niveles no se pretende evitar la resolución de incidencias mediante el escalado de la incidencia, sino lograr la resolución de la incidencia por el personal adecuado.
- Definir Acuerdos de Niveles de Operación (OLA): se trata de crear unos procedimientos técnicos fácilmente entendibles por el Dpto. TI para ofrecer soporte al cliente. En ocasiones, un OLA puede dar soporte a varios SLA.
- Monitorización del cumplimiento de Niveles de Servicios y Acuerdos: mediante este objetivo se pueden cumplir varios cometidos, como el control de calidad de los niveles de servicio o la posibilidad de mejorar o modificar ciertos servicios TI ofrecidos. También se revisa el correcto cumplimiento de proveedores externos.

Obj. Control	Descripción
Definir portfolio de servicios de TI	Se acuerdan y definen los servicios TI de los cuales va a verse beneficiado el Negocio.
Acuerdos de Niveles de Servicio	Se establecen los Acuerdos de Niveles de Servicio entre usuarios y Dpto. TI
Acuerdos de Nivel de Operación	Se definen los acuerdos de Nivel de Operación, que pueden cubrir varios Niveles de Servicio.

Monitorización del cumplimiento de niveles de Servicio y Acuerdos	Proceso de control del correcto cumplimiento de niveles de servicio y acuerdos (internos y externos)

Tabla 12 - Proceso DS1

2.- Administrar los servicios de terceros – DS2

Entendemos por "*terceros"* todas aquellas empresas externas a la compañía que ofrecen servicios de TI o relacionados con el negocio (gestión documental, telecomunicaciones, proveedores de hardware, etc).

- Administrar relación con proveedores: Se analizan y clasifican los proveedores según los servicios que aportan a la compañía. Y se clasifican según su criticidad para la continuidad del negocio.
- Gestionar riesgos de proveedores: se definen los contratos de confianza, continuidad del servicio, penalizaciones en caso de incumplimiento, protocolos a seguir en caso de interrupción del servicio.
- Análisis del desempeño del proveedor: verificar que se aplican las cláusulas estipuladas en el contrato, comprobar que se está manteniendo la calidad del servicio prestado en función de lo acordado en los contratos.

Obj. Control	Descripción
Administrar relaciones con proveedores	Los proveedores se analizarán y clasificarán según los servicios contratados.
Gestión de riesgos	Definición de contratos de continuidad de servicios y procedimientos en caso de interrupción.
Evaluación de competencias	Definir un plan de evaluación de los servicios prestados por terceros.

Tabla 13 - Proceso DS2

3.- Administrar el desempeño y la capacidad – DS3

Este proceso gestiona el desempeño y la capacidad de los **recursos** TI mediante análisis periódicos de su funcionamiento; y de la capacidad de carga de trabajo tanto actual como futura, basándose en una estimación de la dirección estratégica del negocio. El objetivo es asegurar que los recursos de TI son capaces de ofrecer un soporte continuado a las necesidades del negocio.

- Plan de análisis de recursos TI: definir los procesos para realizar el desempeño y analizar la capacidad de los recursos TI frente a las necesidades del negocio. Gestionar el uso de estos elementos evitando entorpecer la labor diaria del personal.
- Administrar capacidad y desempeño: tras la identificación de los recursos TI críticos para la continuidad del negocio, éstos han de ser analizados mediante procesos a seguir con una frecuencia determinada en el plan de análisis.
- Proporcionar continuidad de recursos: cuando por circunstancias del estado de los recursos TI éstos no puedan ofrecer una correcta usabilidad, se han de facilitar los medios para que el usuario no pierda ritmo de trabajo.

Obj. Control	Descripción
Plan de estudio de recursos TI	Analizar el desempeño y la capacidad de los recursos TI de entrega de servicio al negocio.
Administración de capacidad y desempeño	Vigilar su actividad mediante unos procesos regulares
Continuidad de uso de recursos	Proporcionar medios y soluciones que permitan la continuidad del negocio.

Tabla 14 - Proceso DS3

4.- Garantizar la continuidad del servicio – DS4

Tras el proceso que garantiza la continuidad de los recursos TI, éste realiza lo mismo pero con un enfoque más orientado a la gestión del **servicio** TI prestado a los usuarios. En este proceso se realizan todos los controles de personal, infraestructura y proveedores para que, en caso de algún fallo, se pueda

continuar con el desarrollo del negocio. Tan importante es la implantación de nuevos servicios e infraestructura TI como desarrollar planes y protocolos de continuidad de estos elementos para que el negocio no se vea afectado en caso de interrupción o falta de servicio.

Como principales objetivos de control se plantean los siguientes:

- Definición marco de trabajo: en él se determinarán los aspectos claves para la continuación del negocio frente a posibles imprevistos en el funcionamiento de los SI de la compañía. Se definen unos procesos a seguir en función de la infraestructura, roles del personal, tareas y responsabilidades.
- Puntos críticos del sistema: identificación y monitorización de los puntos críticos del sistema que puedan causar una parada del negocio. Asimismo se informará de la disponibilidad de elementos críticos y alternativas de uso.
- Plan de continuidad: diseñado para disminuir el impacto en el negocio en caso de fallo generalizado de SI. Procesar la resistencia y capacidad de recuperación de la infraestructura TI de la empresa.
- Administrar recursos críticos: identificar los recursos críticos para centrar un plan específico de resistencia y recuperación. De este modo se centrarán los esfuerzos y recursos en recuperar los elementos críticos del sistema TI sin desperdiciar tiempo y recursos en recuperar otros menos críticos. También se evalúa el coste de recuperación, para mantenerlo equilibrado y verificar que está entre los costes estipulados de aquellos contratos de servicios firmados con terceros.
- Administración de plan de continuidad de TI: definir un plan de continuidad de TI en función de la infraestructura presente en la empresa. Este plan de continuidad ha de aprobarse según un calendario determinado en el marco de trabajo del plan de continuidad para asegurar que sigue vigente y los empleados tienen los conocimientos suficientes para ejecutarlo. Dicho plan se reparte entre las distintas áreas de TI y de negocio que lo necesiten, así como entre los distintos miembros del Dpto. TI según sus puestos y responsabilidades.
- Recuperar y reanudar servicios de TI: entran en juego varios actores (clientes, empleados de TI y usuarios de negocio). Se han de reactivar los sistemas TI de soporte de datos y recuperación, sistemas de seguridad; se comunica a los usuarios de negocio los tiempos de recuperación y en caso de necesidad, se les comunica a los clientes la situación de recuperación del negocio para que sean conscientes.

- Gestión de respaldos: definir un plan de respaldo de datos y software. Gestionar la ubicación de estos respaldos para asegurarlos frente a fallos de seguridad. Del mismo modo, clasificar el software según su procedencia (hecho a medida o adquirido) para contactar con la empresa desarrolladora y recuperar el software.
- Verificación de la reanudación de sistemas TI: tras el proceso de recuperación del sistema TI, se ha de comprobar que el proceso se ha realizado correctamente, analizando que la totalidad de los datos han sido restablecidos y que el funcionamiento del software es el adecuado. Se analiza el coste (tiempo, personas, monetario) para comprobar que el plan de continuidad de TI está actualizado o necesita renovarse.

Obj. Control	Descripción
Definición marco de trabajo para continuidad de trabajo	Identificar aspectos claves de TI para la continuidad de Negocio. Organizar roles, responsabilidades, personal responsable.
Definición de puntos críticos del sistema	Detectar elementos de infraestructura TI críticos del negocio.
Diseño de plan de continuidad	Definir un plan de continuidad del negocio en caso de fallo generalizado de los sistemas TI.
Gestión de recursos críticos	Identificar y gestionar aquellos recursos TI que sean necesarios para la continuidad del negocio
Administración de plan de continuidad	Definir un calendario de pruebas, identificar roles y responsabilidades.
Recuperación y reinicio de servicios de TI	Procesos y protocolos a seguir durante una parada de sistemas TI.
Gestión de respaldos	Gestionar los distintos *backup* de datos y software del negocio.
Certificación de la reactivación de servicios TI	Comprobar que la recuperación del sistema fue exitosa. Analizar si procede modificar el plan de continuidad.

Tabla 15 – Proceso DS4

5.- Garantizar la seguridad de los sistemas – DS5

Este proceso tiene como finalidad asegurar la integridad de los activos y datos de TI necesarios para la continuidad del negocio: definición de usuarios, claves de acceso, protección de dispositivos, transmisión de datos sensitivos, etc. Implica tanto a usuarios finales como a empleados del dpto. de TI.

- Definir un plan de seguridad de TI: en función de la infraestructura del negocio, los riesgos y el cumplimiento de la normativa existente, se establece un plan de seguridad que vaya alineado con el negocio y la cultura de seguridad de la empresa. Se definen niveles de seguridad según el personal implicado en la seguridad de los sistemas.
- Administrar identidades: asegurar que todos los empleados que estén trabajando en la empresa tengan una identificación única en los sistemas de TI. Se verifica que los accesos y permisos para estos empleados (internos, externos, temporales) está en consonancia con sus funciones y roles. Gestión de estas identificaciones (solicitud, revocación).
- Administrar cuentas de usuario: administrar todo lo relacionado con el alta, bloqueo, borrado y mantenimiento de cuentas de usuario para su uso en los sistemas de TI de la empresa. Determinar los roles y responsabilidades del personal de TI encargado de gestionar los accesos a las aplicaciones bajo su supervisión.
- Monitorización de la Seguridad TI: mediante el control y la supervisión del uso de las herramientas de TI, se vigila que la implementación de la Seguridad TI sea correcta y válida.
- Identificar escenario de brecha de Seguridad TI: comunicar a los usuarios de herramientas TI todas las posibles situaciones de falla de seguridad TI para que tengan los conocimientos necesarios y sepan reaccionar sabiendo las medidas a tomar.
- Fortaleza frente a Software malicioso: tanto usuarios finales como empleados del Dpto. TI han de ser capaces de gestionar software malicioso. Los usuarios finales necesitan recibir información sobre cómo proceder ante algunos escenarios de software malicioso. Los empleados del Dpto. TI tienen que ser capaces de prevenir y detectar la existencia de este tipo de programas malignos para el negocio.
- Seguridad en la red: asegurar el correcto funcionamiento de la red interna del negocio, estructurando la red según necesidades de los usuarios. Fortalecer la red mediante accesos con claves que se renueven con frecuencia. Analizar la red para detectar usos no autorizados.
- Intercambio de datos sensitivos: por la naturaleza del negocio de un bufete, hay un gran flujo de comunicación entre cliente y empleados del negocio. Se ha de asegurar la comunicación,

controlando el envío, el canal de comunicación, verificando la recepción del destinatario, etc. Lo mismo sucede con la comunicación interna dentro de la empresa.

Obj. Control	Descripción
Definición de plan de seguridad TI	Establecer un plan de seguridad alineado con el negocio, en base a la infraestructura TI, usuarios, roles, funciones, etc.
Administración de identidades	Identificar de forma unívoca el uso de los sistemas TI para cada usuario.
Gestión de cuentas de usuarios	Gestión integral de cuentas de usuarios para el eso de aplicaciones del negocio (altas, bajas, modificaciones, suspensiones, etc)
Monitorización de la seguridad TI	Comprobar que la implementación del plan de seguridad es correcto y funciona según lo previsto.
Identificación de escenarios de fallos de seguridad	Definir y planear posibles escenarios de fallos de seguridad para saber cómo actuar frente a esas situaciones.
Fortaleza frente a software malicioso	Securizar los recursos TI del negocio frente a software malicioso. Recuperación del entorno TI del negocio tras un ataque y posterior actualización del sistema de prevención.
Seguridad en red	Establecer parámetros de seguridad dentro de la red interna del negocio.
Asegurar intercambio de datos sensitivos	Asegurar la comunicación de datos sensitivo mediante la involucración del cliente final.

Tabla 16 - Proceso DS5

6.- Educar y entrenar a los usuarios – DS7

Hoy en día la gran mayoría de usuarios tiene o suele tener conocimientos básicos de herramientas de ofimáticas. Sin embargo, cada empresa tiene su propio portfolio de aplicaciones para las cuales son necesarios unos conocimientos de manejo específicos. Lo mismo sucede con el manejo de ciertas herramientas TI para las cuales es necesaria una formación previa a su uso. Este proceso está enfocado en el entrenamiento y la formación en el uso de los SI de la compañía, dirigido a los usuarios finales. Esta formación alcanza desde el propio manejo de los aplicativos en los primeros días de uso hasta la

propia seguridad en el uso genérico de los SI de la compañía. Esto implica varios objetivos de control que paso a detallar a continuación.

- Identificar las necesidades formativas del usuario: en conjunción con la directiva del negocio, el Dpto. TI adecúa la formación necesaria para el aplicativo, trata de identificar los requerimientos actuales y futuros que pueda haber en el negocio y se definen los métodos de impartición.
- Impartición del entrenamiento: tras analizar el objetivo de la formación, se identifican canales de formación, el grupo objetivo, instructores y calendario de formación, y proceso de evaluación final.
- Definir grupos objetivo de la formación: por la existencia de distintos niveles en la jerarquía de la compañía y de distintas tareas, cada usuario puede englobarse en un grupo que recibirá una determinada formación de cara a los recursos y tareas que vaya a realizar, así como en función de los tipos de datos que gestione.
- Evaluación del entrenamiento: para detectar posibles fallos o mejoras en el proceso formativo, se analiza todo el proceso formativo, evaluando todos los actores que han intervenido en la formación. Por otra parte, sirve para determinar si el receptor de la formación aplica correctamente los conocimientos recibidos.

Obj. Control	Descripción
Identificar necesidades formativas	La dirección de negocio y el Dpto. TI se unen para definir las necesidades formativas de un grupo de usuarios finales.
Impartición de la formación	Tras definir las necesidades de conocimientos, se definen grupo objetivo, canales de transmisión, instructores, evaluación final.
Identificar grupos objetivo	En función de las herramientas y los datos que vayan a emplear, los usuarios recibirán una formación específica.
Evaluación de la formación	Tras la finalización de la instrucción, se analiza todo el proceso para detectar posibles mejoras o fallos.

Tabla 17 - Proceso DS7

7.- Administrar la mesa de servicio y los incidentes – DS8

La mesa de servicio es un elemento de gran importancia en la empresa. Es la vía de comunicación entre el grupo de usuarios finales y el Dpto. TI para realizar consultas y comunicar incidencias para su resolución. Es necesaria una mesa de servicio bien organizada y formada para dar una respuesta rápida a estos problemas y evitar paradas innecesarias en el negocio. Gracias a una correcta gestión de la mesa de servicio y de todas las funciones incluidas en ella, la administración del negocio puede detectar el origen de un problema repetitivo y atajarlo de raíz.

Dentro de este objetivo de control me gustaría mencionar la diferencia existente entre incidentes y problemas. Un incidente se podría definir como un suceso fortuito que puede causar una parada del sistema o una disminución de la calidad del servicio prestado al usuario. Por otra parte, un problema es un fenómeno que ocurre con relativa frecuencia, formado por varios incidentes y que puede ser identificado y, por lo tanto, solucionado.

Se van a utilizar los siguientes puntos de control para este objetivo de control:

- Creación de mesa de servicios: la Mesa de Servicio es el elemento por el cual usuarios finales y personal del Dpto. TI se comunican. Se define esta mesa de servicio con unas funciones, jerarquías, canales de comunicación y evaluación final, así como con un dimensionamiento acorde al tamaño de la empresa.
- Gestionar incidencias: la gestión de incidencias está formada por los procesos de apertura de incidencias, su registro, el canal de comunicación entre ambas partes, el tratamiento de la incidencia y su cierre.
- Analítica de tendencias: otro fin de esta Mesa de Servicio es realizar un análisis de tendencia. Con "tendencia" se entiende la evolución o repetición de una determinada tipología de incidencias. Mediante este análisis, se puede llegar a detectar el origen de esta falla y proceder a su resolución (ya sea mediante un plan estratégico de TI o un proceso de emergencia).

Obj. Control	Descripción
Definir Mesa de Servicio	Definir una mesa de Servicio sólida para una correcta comunicación entre usuarios finales y Dpto. TI

Gestión de incidencias	Definir los procesos necesarios para administrar el ciclo de vida de las incidencias abiertas por los usuarios de TI.
Analítica de tendencias	Se analiza la evolución de las incidencias, su resolución, para determinar posibles mejoras en el sistema TI de la empresa.

Tabla 18 - Proceso DS8

8.- Administración de los datos – DS11

En un bufete, como en cualquier otra empresa que trabaje con elementos de SI, los datos son un pilar fundamental para el desarrollo de su labor. Lo más importante para un bufete son sus clientes, estando el servicio desarrollado por el bufete enfocado directamente a los clientes; pero por otro lado, el cliente (ya sea jurídico o físico) tiene derecho a que sus datos sean tratados conforme a las leyes de protección de datos. Este proceso tiene por función definir una correcta y sólida administración de los datos para mantener la robustez del almacenamiento, su confidencialidad y la pronta recuperación en caso de interrupción de los SI.

Otro punto importante a tener en cuenta para este proceso es la legislación vigente con respecto a la protección de datos. Tanto el bufete como aquellas empresas externas que almacenen los datos han de permanecer en el mismo marco legal. Es importante separar este proceso *DS11* del proceso de *Monitoreo y Evaluación ME3* que vela por el cumplimiento de la normativa regulatoria que atañe a los datos tratados por el bufete.

- Estimación de requerimientos: la administración de los datos ha de alinearse con las necesidades del Negocio. Por eso se realiza un acuerdo previo de los datos que se van a gestionar, cómo se almacenarán, en qué ubicación, durante cuánto tiempo. Se identificará la gestión externa de datos, qué datos serán almacenados externamente, así como los acuerdos con terceros para este fin.
- Acuerdos de almacenamiento: definir las condiciones bajo las cuales una empresa externa se encargará de almacenar y custodiar la información de la empresa.
- Respaldo y restauración: establecer los procedimientos a seguir para el respaldo y restauración de los datos tras la interrupción del sistema o la pérdida de datos. La restauración de los datos podrá realizarse desde una ubicación interna de la empresa o acudiendo a la empresa externa

con la que se tenga el acuerdo de almacenaje de datos. En línea con el plan de continuidad acordado en puntos anteriores, se evaluará la fiabilidad de los datos restablecidos.

- Borrado de datos: este proceso ha de realizarse siguiendo los requerimientos de negocio en relación a los datos sensibles. El borrado debe ser realizado por personal con acceso a este tipo de material o por su creador en acuerdo con su responsable. Se controla que los datos han sido realmente borrados y no podrán ser recuperados.
- Seguridad de datos: definir y establecer los parámetros de seguridad bajo los cuales la compañía realice la gestión y administración de los datos. Desde el momento en que reciba o genere los datos, hasta su eliminación. Se trata de una seguridad externa, en la que se securiza los canales de transmisión, y una seguridad interna, por la que se establecen unos roles y jerarquías dando permisos de acceso a los usuarios finales.

Obj. Control	Descripción
Estimación de requerimientos de Negocio	Alinear las necesidades del negocio con la gestión y administración segura de datos.
Acuerdos de almacenamiento	Acuerdos y condiciones de respaldo de datos con empresas proveedoras de servicios de almacenaje
Respaldo y restauración	Definir los procedimientos de recuperación de los datos salvaguardados en caso de pérdida o fallo de los SI.
Borrado de datos	Asegurar que el borrado de datos se hace según los parámetros de seguridad dictados por los parámetros de negocio.
Seguridad de datos	Garantizar la integridad y gestión de los datos

Tabla 19 - Proceso DS11

9.- Administración del ambiente físico – DS12

Este proceso tiene por fin garantizar y asegurar el entorno de trabajo de la infraestructura de TI. Garantizar la seguridad y el control de acceso al entorno de los dispositivos TI para evitar robos, daños o accesos no permitidos a las instalaciones.

- Acceso físico: definir controles de acceso físico a la infraestructura TI de negocio, asignando roles a los empleados de TI correspondientes y determinando la criticidad de las infraestructuras para dotarlas de una seguridad proporcional. Este objetivo de control ha de establecerse en conjunto con el responsable de la monitorización de la infraestructura física y el responsable del negocio (por ende, el dueño de los datos).
- Administración de instalaciones físicas: administración de la infraestructura de TI, como los dispositivos de comunicaciones o los elementos del suministro de energía.
- Medidas de seguridad física: establecer parámetros de seguridad de los elementos físicos de la infraestructura TI en las dependencias de la empresa.

Obj. Control	Descripción
Acceso físico y disposición de elementos TI	Administrar y controlas los accesos a dependencias en donde se encuentren dispositivos de TI.
Administración de instalaciones físicas	Administración de la infraestructura de TI
Medidas de seguridad física	Definir parámetros de seguridad de los elementos físicos de TI.

Tabla 20 - Proceso DS12

10.- Administración de operaciones – DS13

Por Administración de operaciones, se entiende la gestión de operaciones que afectan a la infraestructura que soporta el funcionamiento TI del Negocio. Se trata de mantener la integridad de los datos (evitar que sean borrados o eliminados por error o sustraídos) y asegurar el correcto funcionamiento de la infraestructura TI y su salvaguarda de tal forma que se interfiera lo menos posibles en el correcto funcionamiento del negocio. Está enfocado a soportar los procesos de negocio, mediante el análisis del funcionamiento de la infraestructura TI para ser capaz de prevenir posibles fallas o riesgos.

Como puntos de control enumero los siguientes:

- Programación de tareas: organizar y programar todas las tareas relativas a la gestión y uso de elementos de TI. De este modo se puede conseguir una optimización de los recursos al realizar

ciertas tareas sin intervenir en el uso cotidiano de estos recursos por parte de los usuarios. Se trata de disminuir en la medida de lo posible el impacto en el negocio.

- Documentos sensitivos y dispositivos de salida: este punto de control se centra en la salvaguarda de datos sensibles y material de uso especial.
- Mantenimiento preventivo del hardware: vigilar el uso y rendimiento de las infraestructuras TI para detectar posibles problemas y poder tratarlos a tiempo. O en caso de no tener solución, prever de antemano una sustitución del material para no interrumpir el negocio.

Obj. Control	Descripción
Programación de tareas	Diseñar un calendario para la ejecución de ciertas tareas de gestión de elementos TI.
Información sensible / dispositivos de salida	Protección de los datos sensibles y la infraestructura TI de uso especial
Mantenimiento preventivo	Tareas de análisis para prever problemas en la infraestructura TI de la compañía.

Tabla 21 - Proceso DS13

IV - Monitorear y evaluar

1.- Monitorear y evaluar el desempeño de TI – ME1

Para asegurarnos de que las acciones del dpto. TI son correctas y están alineadas con el negocio, se hace necesario el uso de acciones de monitoreo y evaluación de su desempeño y labores. Se definen una serie de objetivos de control para evitar el desvío con respecto al negocio.

- Disminuir el número de riesgos que se convierten en problemas: Se busca identificar todos los posibles riesgos que atañan al ámbito TI para evitar que se transformen en problemas cuando se emplee ese elemento TI a la hora de entregar el servicio al cliente.
- Cumplir con los plazos de entrega de servicios: los servicios TI ofrecidos han de ejecutarse en el tiempo estipulado en los planes estratégicos de TI. Cualquier retraso podría incurrir en penalizaciones económicas o pérdida de imagen de cara al cliente.

- Definir revisiones periódicas: analizar la existencia de problemas en los servicios de TI para corregir el origen de estos problemas con una determinada frecuencia. La corrección del problema consiste en encontrar los factores de riesgo que desembocan en ese problema.
- Definición de objetivos de desempeño: en conjunto con la gerencia de cada departamento, la directiva de negocio y los usuarios, se establece una colección de referencias con las que comparar los objetivos a cumplir para lograr así una adecuada medición del desempeño de los SI de la empresa.

Obj. Control	Descripción
Disminución de riesgos/problemas	Reducir los riesgos TI que se transforman en problemas para los servicios entregados al cliente.
Cumplir plazos de entrega de servicios	Establecer y cumplir los plazos de los servicios TI.
Ejecución periódica de análisis de TI	Análisis y estudio del problema del servicio TI para su corrección.
Definir objetivos de desempeño	Para determinar el correcto desempeño de los recursos y servicios TI, se determinan una serie de objetivos de desempeño que son analizados.

Tabla 22 - Proceso ME1

2.- Garantizar el cumplimiento regulatorio – ME3

Existen una serie de normas, regulaciones y leyes que atañen al uso de las tecnologías y datos de los SI que la empresa ha de cumplir. Es por ello que hay que definir un marco de trabajo que identifique bajo qué normas y regulaciones se mueve el negocio de la empresa, comprobar que se estén aplicando correctamente, corregir el negocio en caso de desviación con respecto a estas normas y establecer los procedimientos necesarios para asegurar el cumplimiento de estas normativas.

- Identificación de las normativas aplicables: identificar las normativas y regulaciones que se aplican a la operativa de la empresa sobre la gestión de TI y SI.

- Revisión y ajuste de los procedimientos TI: localizar y analizar todos los procesos cuyo funcionamiento esté supervisado por alguna de estas normativas.
- Garantizar cumplimiento de normativas: tras identificar todos estos procesos, se realiza la comprobación de que están alineados con el cumplimiento de las normativas de TI y se persigue que su funcionamiento continúe en esa línea operativa.

Obj. Control	Descripción
Identificación de normativas aplicables al Negocio	Identificar normativas y regulaciones respecto a los procesos TI
Revisión y ajustes de procesos TI	Análisis del funcionamiento de los procesos TI en relación con la normativa aplicable
Garantizar y mantener cumplimiento de normativas	Asegurar el correcto funcionamiento de las TI en consonancia con la normativa de SI.

Tabla 23 - Proceso ME3

4.- Elaboración de un marco de trabajo basado en COBIT

Alcance de la auditoría

Dimensionamiento

Se trata de un bufete de tamaño medio, compuesto por unos 20 miembros. Inicialmente el germen de la firma estaba compuesto por una oficina en Madrid, dirigida por tres socios y cuyas tareas son realizadas por un grupo de unos 20 abogados especializados en diversos ámbitos como Fiscal, Mercantil, Inmobiliaria, Civil, Arbitrajes, Penal y la gestión de grandes fortunas. Para dar soporte a esta operativa, cuentan con el apoyo de un departamento de administración, dentro de cual se incluye el personal de RRHH, administración y la persona encargada del soporte técnico de TI.

El motivo de esta extraña relación entre el Dpto. TI (compuesto por un empleado) es que uno de los socios es el encargado de la gestión y administración del Dpto. TI. Dicho departamento está directamente subordinado a él, aunque los usuarios que demanden atención técnica pueden acudir a él mediante los canales de comunicación correspondientes.

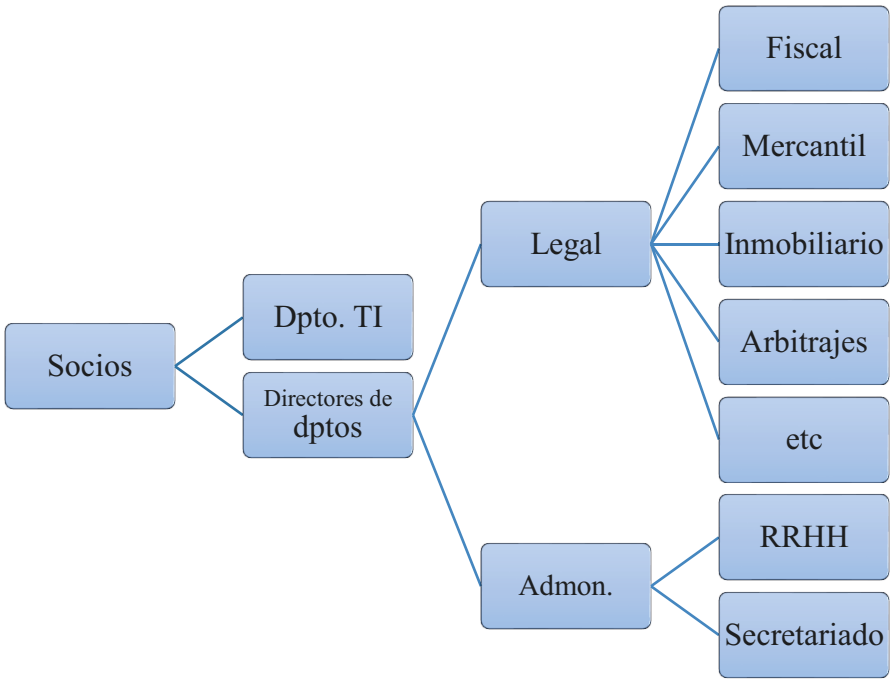


Figura 9 - Marco Organizativo

En la actualidad, la firma ha ampliado su operativa ayudándose en unas oficinas ubicadas en Málaga, Pontevedra y en Moscú para dar respuesta a la clientela internacional.

Operativa del bufete

Como en la mayoría de los bufetes –así como en el resto de PyME's- la inclusión de las TI para la ejecución de su operativa ha ido en aumento hasta convertirse en un activo clave para la consecución de sus objetivos. Estamos frente a la operativa de un bufete, que tradicionalmente podría considerarse manual. No estamos en una consultora financiera que ha de generar y tratar grandes cantidades económicas, analizarlas y tomar decisiones en base a los datos; la operativa de un bufete se basa más en la realización de escritos judiciales, redacción de contratos, recursos, relación con clientes.

Por lo tanto la principal necesidad que tiene el bufete con respecto a las TI es la gestión de datos, entendiendo por *datos*, toda la documentación generada dentro del bufete y toda aquella que recibe y envía desde/a organismos externos y sus clientes; y por otra parte, el almacenamiento de información que ha de mantener la fiabilidad e integridad.

Infraestructura TIC

Se trata de un bufete de reducidas dimensiones, tanto en cuanto a personal como en lo relativo a las instalaciones. Está ubicado en un bloque de pisos de la zona centro de Madrid. Compuesto por los dos únicos apartamentos que hay en cada rellano. Tienen por lo tanto dos entradas principales y dos entradas traseras en el rellano de la escalera de servicio que están abiertas y por las cuales los empleados pueden pasar. Estas entradas quedan separadas de las escaleras mediante un biombo de madera No poseen un gran centro de datos, ni potentes servidores para almacenar la información con la que operan. Trabajan principalmente con ordenadores portátiles *mini* cuya misión es otorgar al bufete una imagen de empresa moderna y evolucionada tecnológicamente y por otra parte, para facilitar el movimiento a sus abogados. Resulta más cómodo desplazarse al cliente con un pequeño portátil de dimensiones y peso reducido, que tener que cargar con un "portátil" pesado de 15,4".

Para el uso y disposición de datos, así como almacenaje, el bufete usaba un ordenador de sobremesa cedido por uno de los socios, con un sistema operativo Windows Vista. Contra él estaban conectados

todos los ordenadores portátiles de los abogados y los sobremesas de los empleados del dpto. de administración. A este ordenador también van dirigidos los faxes recibidos que se guardan en formato PDF. Con el paso del tiempo, se adquirió otro sobremesa que se ubicó en el otro piso a modo de servidor central (con Windows Server 2008), conectado a este primer sobremesa para realizar las copias de seguridad.

Por otra parte, existen una serie de dispositivos y periféricos de uso común a los cuales tienen acceso varios o todos los usuarios, según sus necesidades y perfiles en la jerarquía de la compañía. Estos dispositivos son impresoras que algunos usuarios tienen en sus propios despachos para uso personal y otras disponibles en espacios comunes, escáneres y el fax del despacho.

Para finalizar, cada empleado dispone de unos periféricos conectados a su portátil cuando ha de trabajar en las oficinas. Un monitor o dos según el empleado, teclado y ratón, dispositivos de memoria externa que también serán objeto de análisis.

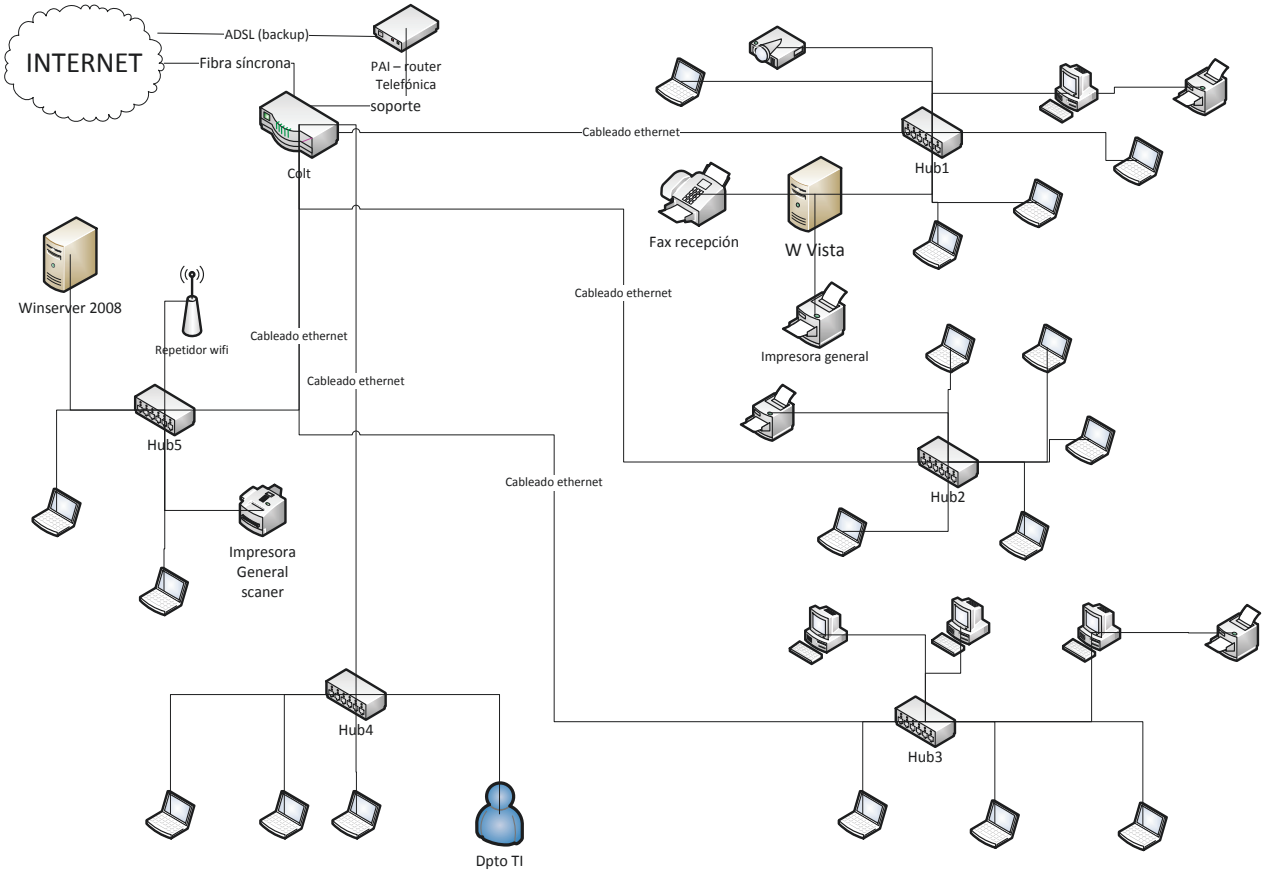


Figura 10 - Estructura TIC del bufete

El nivel de externalización de servicios TI es bajo basándose en la compañía Colt como proveedora de fibra óptica para la conexión al exterior, así como del proceso de instalación y montaje de toda la red interna del despacho. Telefónica les provee la conexión ADSL que se emplea en caso de caída de red de Colt, usando el router como balanceador de carga. Para el servicio de almacenaje y sincronización de ficheros, el bufete ha recurrido a una empresa *online* con buena reputación, SugarSync. Entre el servicio básico de sincronización de ficheros, SugarSync permite trabajar de forma colaborativa, así como acceder desde cualquier dispositivo desde cualquier lugar.

En lo relativo al soporte de dispositivos, mantienen una garantía con HP para el mantenimiento y reparaciones de los portátiles y una empresa de servicio técnico certificado por Konica les proporciona soporte y factura por el alquiler y uso de la impresora general.

Alcance de la ASI

Mi intención es la de tomar todos los objetivos de control de CObIT que he considerado aptos para el bufete como hoja de ruta o *checklist* que permita guiar al auditor en el proceso de realización de una Auditoría de Sistemas de la Información. Se basará en la observación y varias encuestas sobre la operatividad de los empleados con respecto a las TIC de la empresa para determinar los riesgos TI del Negocio. En función de estos resultados, se expondrían una serie de mejoras y buenas prácticas que redundarían en un beneficio para el negocio, seguridad en su infraestructura TI, fiabilidad de los datos y una mayor calidad en el servicio ofertado a la clientela.

Objetivos del Dpto. TI

Tras la descripción de la operativa realizada por el bufete, así como de su estructura organizativa y de SI, paso a enumerar los objetivos que tiene el departamento de TIC siempre buscando satisfacer los objetivos de negocio de la empresa, tanto directa como indirectamente:

- Dar Soporte técnico a usuarios: resolución de incidencias, análisis de problemas para su posterior solución.
- Desarrollar servicios TI: diseño y mantenimiento del portal web del negocio, así como el desarrollo de una aplicación para la gestión de incurridos (gastos y horas imputables al cliente).

- Formación: en función de las necesidades del negocio con respecto al manejo de recursos TI, el dpto. TI se encarga de elaborar unos documentos informativos y desarrollar una serie de recursos lectivos para aleccionar correctamente a los usuarios.
- Mantener la red interna operativa: Mientras que la instalación ha sido realizad por empresas proveedoras de servicios de comunicaciones, el mantenimiento de la infraestructura de red interna queda a cargo del dpto. TI.
- Mantener la infraestructura TI del bufete: mantener en correcto funcionamiento los servidores y tramitar los acuerdos de garantía con los proveedores de los ordenadores, servidores, impresoras. Así mismo, comprobar el correcto funcionamiento de dispositivos como el fax y el escáner.

Base de análisis y controles

Como ya expliqué anteriormente, la finalidad de este proyecto no está en realizar una auditoría propiamente dicha de este bufete, sino la de fabricar una base de análisis y controles sobre el bufete que puedan servir a una futura auditoría informática. Basándome en CObIT y dividiendo todo lo que abarca TI en varios grupos, iré aplicando los objetivos de control para determinar los puntos de la *checklist.*

El plan de auditoría se basa en analizar las siguientes áreas de la compañía, que son aquellas que están en contacto directo y dependen del buen uso de las TIC:

- Planear y organizar: en un bufete de estas dimensiones con un departamento de TI compuesto por una sola persona, este dominio de CObIT tiene muy poca aplicación, salvo los procesos básicos necesarios para administrar los elementos necesarios para el correcto funcionamiento de TI. Un plan estratégico que defina y estructura su funcionamiento y la relación con el cliente (en este caso los usuarios), la administración de los recursos TI (entendiendo los recursos TI como la parte humana y lógica/física del dpto. TI), los posibles riesgos a los que se enfrenta la gestión de TI y por último, pero igual de importante, la gestión de la inversión en los recursos TI.
- Adquirir e Implementar: es el dominio que engloba los procesos encargados de la adquisición de recursos TI necesarios para el correcto desempeño del negocio por parte de los usuarios y sobre todo, de su mantenimiento, que debido a la actividad frenética de este tipo de negocio, supone un elemento crítico. Se asegura que los productos respondan a las necesidades de los

usuarios y que los cambios en ellos no afecten al rendimiento del personal ni a la imagen de la compañía.

- Entregar y dar soporte: bajo este dominio tienen cabida los distintos procesos que gestionan la operativa relacionada con la entrega de nuevos elementos de TI y su posterior soporte a los usuarios. Este soporte a usuarios está constituido por la evaluación de estos servicios y el consiguiente servicio de atención al usuario en caso de alguna incidencia. Creo que este bloque de CObIT es uno de los más importantes. Estamos frente a unos objetivos de control que aseguran que el día a día de la funcionalidad de los elementos TI del negocio funcione correctamente, con los niveles de calidad estipulados y según lo acordado entre Negocio y el Dpto. TI.
- Monitorear y Evaluar: este dominio está enfocado a la supervisión y vigilancia de la infraestructura TI para tratar de detectar problemas antes de que sucedan y puedan causar daños al negocio. Enfocado al mismo resultado, evitar daños a la imagen del negocio y que no sea multado, también se vigila el cumplimiento regulatorio de la gestión de los datos que manipula en la operativa diaria.

Para desarrollar la puesta en marcha práctica de estos procesos de CObIT, se determinarán una serie de métricas a tomar en consideración para definir si los objetivos de control de los procesos se cumplen. La valoración de estas métricas [*metr*] nos ayuda a determinar los elementos a mejorar tras la auditoría en aras de mejorar el Gobierno de TI de la compañía. Para calcular los valores de estas métricas se pueden recurrir a técnicas como los cuestionarios a los distintos usuarios involucrados en este proceso, o a la mera observación y análisis por parte del auditor informático de los recursos TI de la empresa.

Selección de procesos CObIT

CObIT es un amplio y vasto conjunto de procesos de evaluación, monitorización, análisis aplicable a multitud de empresas, definido y acordado por varios profesionales de ISACA. Sin embargo, para la aplicación real al bufete en donde desempeñé mis prácticas, analicé la aplicación y el provecho que se le podría sacar a todos los procesos como base para una futura auditoría informática y tomé la decisión de desechar algunos procesos.

Por ejemplo, estimé que procesos como "*PO3 – Determinar la dirección tecnológica"* no tenían sentido dado el uso que se hace de las TIC. Otros procesos como el "*PO4 – Definir los procesos, Organización y Relaciones de TI"* tendrían mayor cabida en empresas de mayor tamaño.

En el grupo de procesos de *Adquisición e Implantación* sólo tuve en cuenta aquellos procesos que por el funcionamiento de la empresa tenían sentido elegir. Desestimé el proceso *"AI7 – Instalar y acreditar soluciones y cambios"* porque los servicios TI que se desarrollan en este bufete no necesitan de este proceso.

Sin embargo, en lo relativo a los procesos de *"Entregar y dar soporte"* y *"Monitorear y evaluar*" sí he tenido en cuenta más procesos. Creo que de cara al trabajo que realiza el Dpto. TI de un bufete de este tamaño, son más útiles y su correcta implementación puede favorecer en gran medida a los logros del negocio.

Proceso PO1

Este proceso es un elemento difícil de analizar mediante la simple observación, por lo tanto habrá que realizar un cuestionario a aquellos actores implicados.

Cuestión	Persona implicada
¿Existe un plan centrado en la gestión de TI en la empresa?	Socio(s) del bufete Cuerpo directivo del bufete
¿Conoce la existencia de un plan de gestión de TI?	Responsable dpto. TI

Tabla 24 - Cuestionario PO1

Analizar los resultados de las siguientes métricas para determinar la correcta consecución de este proceso:

- % de procesos TI reflejados en el plan estratégico TI
- # de usuarios que conocen el plan estratégico TI
- Frecuencia de revisión del plan estratégica TI

Proceso PO2

Cuestionario empleado para este proceso:

Cuestión	Persona implicada
¿Está definida la gestión de datos en el plan de TI de la empresa?	Responsable TI
¿Conoce cómo ha de nombrar los distintos tipos de archivos?	Usuario final
¿Conoce en qué ubicación se encuentran los ficheros que necesita?	Usuario final
¿Se ha encontrado con algún fichero correctamente nombrado con contenido erróneo?	Usuario final

Tabla 25 - Cuestionario PO2

Métricas a emplear para determinar la correcta ejecución de este proceso:

- # de tipo de datos sin nombrado asignado en el plan.
- Tiempo medio empleado por el usuario en localizar los ficheros.
- # de ficheros hallados en los servidores con nombrado incorrecto
- % de ficheros/datos redundantes
- # de tipos de datos no corresponden con su finalidad
- # de ficheros con información sensible almacenados incorrectamente
- # de ficheros con contenido no relacionado con su nomenclatura

Proceso PO5

Cuestionario a realizar a los empleados:

Cuestión	Persona implicada
¿Está incluido en la gestión de costes un apartado para los costes de TI?	Directiva de la empresa

¿Existe alguna relación entre la inversión en TI y la obtención de resultados de negocio?	Directiva de la empresa
¿Ha mejorado el rendimiento de la empresa con las últimas inversiones realizadas en TI	Directiva de la empresa
¿Considera que la labores diarias relacionadas con TI son más livianas	Empleado
¿Se ha tenido en cuenta sus recomendaciones a la gerencia	Dpto. TI
¿Tiene inventariado los equipos y etiquetados los soportes externos?	Dpto. TI

Tabla 26 - Cuestionario PO5

Métricas para el análisis de este proceso:

- Desviación entre la inversión programada y el coste de TI
- Relación entre la inversión en TI y los beneficios reportados por los servicios TI

Proceso PO7

Preguntas dirigidas al personal de la empresa:

Cuestión	Persona implicada
¿Existe una guía de cuestiones técnicas al entrevistado?	Directiva administración
¿El personal de RRHH dispone de la formación técnica suficiente para afrontar la entrevista?	Directiva administración
¿El personal de TI conoce sus labores?	Directiva TI

Tabla 27 - Cuestionario PO7

Métricas para analizar el cumplimiento de este proceso:

- # de CV recibidos de candidatos

- # de anuncios publicados
- % de los CV recibidos entre cada canal de comunicación de RRHH
- # de CV's localizados en ubicaciones erróneas
- # de quejas sobre Dpto. TI recibidas por parte de usuarios
- % de procesos TI documentados
- # de cursos de formación TI impartidos

Proceso PO9

Cuestionario a realizar por el auditor

Cuestión	Persona implicada
¿Existe un plan de identificación de riesgos TI?	Directiva Negocio
¿Es capaz de identificar situaciones de riesgo TI?	Usuarios
¿Sabe cómo reaccionar ante una situación de riesgo TI?	Usuarios

Tabla 28 - Cuestionario PO9

Métricas a calcular:

- # de eventos críticos no identificados en el plan de evaluación de riesgos
- # de eventos críticos cubiertos por plan de continuidad
- % de situaciones críticas no resueltas satisfactoriamente
- Costes derivados de las penalizaciones derivadas de las situaciones críticas no resueltas

Proceso PO10

Nos encontramos frente a una empresa en la cual la existencia de "proyecto TI", tal y como se concibe en el mundo informático, es escasa. Uno de los principales proyectos presente es el desarrollo y mantenimiento del portal web. El resto de procesos relacionados con la TI, son de corta duración y no incluyen los pasos característicos de un proyecto TI.

Cuestionario:

Cuestión	Persona implicada
¿Existe una política estructurada para proyectos TI	Dirección
¿Los usuarios conocen los proyectos TI actualmente en marcha?	Usuarios
¿La definición y alcance de los proyectos TI está definida?	Dirección TI
¿El uso de recursos está priorizado correctamente?	Dirección TI

Tabla 29 - Cuestionario PO10

Métricas a calcular:

- # de hitos del proyecto realizados fuera de plazo
- # de tareas adicionales no definidas en la documentación del proyecto
- Tiempo de espera de ejecución de un proyecto por problemas de concurrencia de recursos

Proceso AI1

Dentro de un bufete, la mayoría de los procesos que se realizan son manuales, aún mediante el uso de TIC, es muy importante el factor humano. Existen varias tareas en el día a día del bufete que son repetitivas y metódicas, pero que o bien su coste de automatización sería excesivo, o el riesgo de la dependencia del negocio de este proceso automatizado sería elevado. Hay que realizar un análisis de toda la operativa, ya sea diaria o mensual cuyo balance coste-riesgo permita ser automatizado.

Cuestionario dirigido al personal:

Cuestión	Persona implicada
¿Disponen de un plan detallado de todos los procesos internos en los que intervenga las TI?	Directiva bufete
¿Se han recibido solicitudes de los distintos departamentos para automatizar procesos	Directiva bufete / Dpto. TI

En base a los posibles procesos automatizables ¿se ha realizado un análisis de riesgos?	Directiva Bufete / Dpto. TI
¿De qué manera se realiza la toma de requisitos funcionales y requerimientos técnicos	Dpto. TI

Tabla 30 - Cuestionario AI1

Métricas:

- # de peticiones recibidas para automatizar una tarea.
- % de tiempo invertido por el usuario en una tarea de forma manual
- Grado de riesgo en automatizar un proceso de negocio

Proceso AI2

Dentro de un bufete de abogados existen algunas tareas que por su naturaleza, no pueden ser soportadas por el *software* disponible en el mercado, ya sea por sus limitaciones, por el precio, por el uso de licencias, por diversos motivos. Es por ello que en ocasiones puede ser necesario solicitar a una empresa externa de desarrollo que fabrique para el negocio un aplicativo. Un posible ejemplo en este caso, podría ser el desarrollo de un sistema de gestión documental.

Cuestionario para los usuarios:

Cuestión	Persona implicada
¿Se realizan reuniones periódicas con los usuarios para conocer sus necesidades?	Directiva de negocio
¿Se realiza un análisis previo comparativo del mercado para adquirir software en la oficina?	Directiva de negocio / Dpto. TI
¿Se verifica que el software adquirido cumple con la normativa regulatoria que aplica el bufete?	Directiva de negocio
¿Existe algún plan para la implantación y mantenimiento del software aplicativo?	Dpto. TI

Tabla 31 - Cuestionario AI2

Métricas para determinar que se cumplen estos objetivos:

- # de peticiones extra realizadas tras la finalización de la toma de requisitos.
- % de reducción del tiempo dedicado a una terea mediante el nuevo software aplicativo.
- % de necesidades cubiertas con el software aplicativo.
- # de incidencias reportadas por los usuarios.

Proceso AI3

Una de las situaciones críticas e inesperadas que pueden darse en la vida diaria de un bufete es que un usuario pierda su portátil o éste deje de funcionar. El usuario no puede esperar a que se adquiera otro portátil o esperar a que el servicio técnico restituya el portátil averiado. Se han de tener los medios necesarios para que el usuario no pierda tiempo y este incidente no repercuta en la continuidad de la operativa del bufete. Otros elementos que considero que pueden formar parte de la infraestructura tecnológica de la empresa son las impresoras y fax, para los cuales hay que tener una previsión de repuestos en buen estado.

Cuestionario a realizar:

Cuestión	Persona implicada
¿Existe un plan para adquirir y gestionar elementos de repuesto?	Directiva de negocio
¿Se integran satisfactoriamente los nuevos sistemas en la infraestructura tecnológica actual?	Dpto. TI / Usuarios
¿La integridad, seguridad y disponibilidad de la infraestructura tecnológica es la adecuada?	Dpto. TI
¿Se gestionan correctamente aquellos dispositivos que han terminado su ciclo de vida?	Dpto. TI
¿Se analizan los riesgos al integrar nuevos dispositivos a la infraestructura TI?	Dpto. TI
¿Existe una documentación detallada del proceso de puesta en marcha de los nuevos dispositivos?	Dpto. TI

Tabla 32 - Cuestionario AI3

Métricas empleadas por el auditor:

- # de incidencias presentadas por los usuarios al manejar nuevos dispositivos.
- Duración de la puesta en marcha del recurso de infraestructura tecnológica.
- # de incidencias debido a la falta de previsión de falta de capacidad.
- # de dispositivos con la garantía de fabricante caducada.

Proceso AI4

Como ya se ha mencionado anteriormente, un bufete no es una compañía en donde se realicen desarrollos TI o existan grandes proyectos de productos TI. Sin embargo, sí que una buena parte de su labor se basa en el uso de las TIC. Es por ello que, aun en menor medida, sí es necesario un proceso que se encargue de definir las transferencias de conocimiento a las distintas áreas de negocio. Es importante definir este proceso de enseñanza de tal forma que influya lo menos posible en el rendimiento del receptor. Más adelante se evaluará el proceso que ejecuta esa transferencia. Son quizás dos procesos que pueden parecer muy similares, pero que en el fondo tienen distintas funciones.

Cuestionario:

Cuestión	Persona implicada
¿La formación sobre el manejo de herramientas TI está documentada?	Directiva de negocio Dpto. TI
¿Quién se encarga de elaborar esta documentación?	Directiva de Negocio
¿Existe un proceso por el cual se entregue la formación al usuario?	Dpto. TI
¿La documentación de formación está organizada y enfocada según el tipo de usuario que la recibe?	Dpto. TI
¿La documentación queda disponible para futuras consultas de los usuarios?	Dpto. TI

Tabla 33 - Cuestionario AI4

Métricas para el auditor:

- # de servicios TI cubiertos por la formación.
- Frecuencia de los periodos de formación.
- # de incidentes debido a documentación errónea o falta de ella.
- # de documentos desactualizados.
- # de solicitudes de nueva formación

Proceso AI5

En el caso de un bufete, los recursos de TI necesarios para su correcto funcionamiento son aquellos enfocados a las comunicaciones y el almacenaje de información. En lo relativo a las comunicaciones, el bufete tiene un acuerdo con dos empresas proveedoras: una de ellas le facilita conexión por fibra óptica síncrona y la segunda ofrece una conexión ADSL que el bufete utiliza como soporte en caso de que la primera falle. En lo relativo al almacenaje de datos, el bufete recurre a una empresa de sincronización online (*SugarSync*) mediante la cual los archivos del negocio se almacenan y son accesibles desde cualquier ubicación. Otro recurso de TI a tener en cuenta es el soporte técnico a los equipos que forman parte de la infraestructura TI de la empresa.

Cuestionario para los empleados:

Cuestión	Persona implicada
¿Existen políticas para la adquisición de recursos TI	Directiva de negocio
¿Se realiza algún tipo de análisis comparativo para la adquisición de recursos TI	Directiva de negocio Dpto. TI
¿Qué criterios se siguen en el momento de adquirir los recursos TI	Directiva de negocio Dpto. TI
¿Posteriormente a la adquisición, se realiza algún estudio comparativo con otras ofertas?	Dpto. TI

Tabla 34 - Cuestionario AI5

Métricas proceso AI5:

- # de necesidades del negocio cubiertas por los recursos contratados
- Grado de relación entre inversión en el recurso TI y beneficios obtenidos

Proceso DS1

Una de las funciones más importantes que desempeña el dpto. TI en el corazón del bufete es el soporte técnico a los usuarios. No solo participa en la toma de decisiones con respecto a la gestión y administración de TI dando soporte a la directiva de negocio como hemos visto en anteriores puntos, sino que está disponible para resolver las incidencias técnicas a las que se enfrentan los usuarios. Es por ello que el proceso de definición y administración de los niveles de servicio es crítico y es importante que se realice de forma efectiva. Para comprobar que los objetivos de control se cumplen, he aquí una lista de cuestiones y métricas que el auditor deberá analizar y estimar.

Cuestionario

Cuestión	Persona implicada
¿Existe un plan que defina los servicios prestados por el Dpto. TI?	Directiva de Negocio Dpto. TI
¿Se revisa de forma regular dicho plan de actuación?	Directiva de Negocio
¿Cómo se realiza la petición de soporte por parte del usuario?	Usuarios de recursos TI

Tabla 35 - Cuestionario DS1

Métricas de evaluación:

- % de satisfacción de los usuarios a sus solicitudes.
- Grado de uso de los canales de comunicación con Dpto. TI.
- % de cobertura de los servicios de nivel en respuesta a las peticiones realizadas por parte de usuarios.

Proceso DS2

Este proceso está enfocado a controlar el buen servicio prestado por empresas ajenas al propio bufete. Tal y como mencioné antes, el bufete confía a una serie de proveedores de servicios de TI la gestión de las impresoras y escáner, así como el aprovisionamiento de internet y la gestión y sincronización documental. Para estos casos, este proceso se compone de varios objetivos de control que han de asegurarse mediante los siguientes elementos.

Cuestionario de proceso DS2

Cuestión	Persona implicada
¿Existe algún plan de supervisión de servicios prestados por terceros?	Directiva de negocio Dpto. TI
¿Existe un plan de riesgos para los servicios prestados con terceros	Directiva de negocio Dpto. TI
¿Se realiza un proceso continuado de supervisión de las prestaciones de los proveedores?	Dpto. TI
¿Se revisan de forma periódica los contratos con los proveedores	Directiva de negocio
¿Se realizan revisiones periódicas del desempeño de los proveedores	Dpto. TI
¿Los usuarios conocen los procedimientos en caso de fallo de servicio de proveedor?	Usuarios finales

Tabla 36 - Cuestionario DS2

Métricas de evaluación:

- # de llamadas al proveedor por culpa de un mal servicio
- # de informes realizados sobre el desempeño del proveedor de servicio
- # de paradas de negocio por culpa de un fallo de servicio externo
- % de reembolsos realizados por el proveedor

Proceso DS3

Dentro de un bufete de reducidas dimensiones, es muy fácil estancarse en el funcionamiento de la simple revisión diaria del funcionamiento de los recursos TI y no tratar de ir más allá, y de prever posibles necesidades del negocio para ser capaz de afrontarlas con éxito. Es necesario analizar el actual funcionamiento de los recursos TI y los requerimientos que tienen los usuarios para detectar posibles situaciones de riesgo y ser capaces de afrontarlas y resolverlas con éxito.

Cuestionario:

Cuestión	Persona implicada
¿Se están entregando los servicios de TI en línea con las necesidades del negocio?	Directiva negocio Usuarios
¿Existe algún mecanismo estadístico que permita monitorear el desempeño actual de los procesos TI en el negocio?	Dpto. TI
¿Se realizan reuniones frecuentes para evaluar los incidentes y procesos en los cuales están involucradas las TIC?	Dpto. TI Directiva de negocio
¿Existe un contacto constante con la gerencia para comunicar mejoras sobre los procesos TI?	Dpto. TI Directiva de negocio

Tabla 37 - Cuestionario DS3

Métricas a calcular:

- # de horas de trabajo perdidas por culpa de la poca capacitación de las TI.
- Tiempo de respuesta ante contingencias de los recursos TI.
- Tiempo de respuesta de proveedores externos
- # de servicios TI revisados
- # de actualizaciones de servicios TI (para su mejora)
- Esfuerzo de resolución de problemas
- Tiempo empleado en la identificación de problemas

Proceso DS4

El trabajo dentro de un bufete es frenético, puesto que se factura al cliente por horas trabajadas, los abogados no pueden permitirse el lujo de perder tiempo por culpa de incidencias relacionadas con sus herramientas de trabajo. Eso repercutiría negativamente de cara al cliente. Si sus portátiles dejan de funcionar, o el acceso a los servidores en donde se almacenan los ficheros se corta, necesitan una rápida respuesta del soporte. Del mismo modo que si la conexión telefónica se corta o el fax deja de recibir mensajes, podría suponer un grave problema y ya no sólo económico, sino legal. Mediante este cuestionario y el análisis de las siguientes métricas, se analiza que los objetivos de control de este proceso se cumplan satisfactoriamente.

Cuestionario:

Cuestión	Persona implicada
¿Existe algún plan de continuidad definido dentro de la organización?	Directiva de Negocio Dpto. TI
¿Se tienen identificados los procesos críticos dentro de la estructura organizacional de la empresa?	Directiva de Negocio
¿Se tienen priorizados estos procesos críticos en relación al uso de recursos TI?	Directiva de Negocio Dpto. TI
¿Los usuarios conocen el procedimiento para solventar estos procesos críticos?	Usuario final Dpto. TI
¿Existen sistemas de alimentación ininterrumpida (SAI) para los servidores de la oficina?	Dpto. TI
¿Existe alguna ubicación remota contra la cual se realicen copias de seguridad?	Dpto. TI
¿Se realizan pruebas de continuidad y recuperación?	Dpto. TI
¿Existen medidas de protección anti-incendios? (extintores, detectores de humo, etc)	Directiva de negocio

Tabla 38 - Cuestionario DS4

Métricas a analizar:

- % en uso de la capacidad de almacenaje de los servidores.
- % en uso de la capacidad del servicio de repositorio online.
- # de errores críticos identificados y documentados.
- Tiempo perdido de cada usuario por fallos en las TIC.
- Duración de las interrupciones.
- # de ensayos de recuperación del sistema.
- # de consultas de los usuarios frente a casos de interrupción del sistema.
- # de ficheros de respaldo desactualizados

Proceso DS5

Como en cualquier empresa que maneje información (y más aún en un bufete en donde el contenido de información sensible es grande) es de suma importancia administrar correctamente la seguridad de los sistemas. En el caso de este bufete, es de vital importancia controlar el acceso a las dependencias y los despachos a través de las dos entradas. Una vez en el interior del despacho, la seguridad de cada puesto de trabajo es responsabilidad de su usuario y debe tomar las medidas oportunas que estén en su mano para mantener la seguridad.

Además de las medidas de seguridad que puedan tomar los usuarios, el Dpto. TI del bufete es partícipe también de todos los métodos de seguridad que se puedan aplicar. Su tarea es la de gestionar y administrar esta seguridad de los sistemas en el seno del bufete. No sólo se encarga de los puestos de trabajo, sino también de otros elementos de la infraestructura de SI del bufete como son los servidores o los dispositivos de escáner, fax e impresión.

Cuestionario para revisar los objetivos de control de este proceso:

Cuestión	Persona implicada
¿Qué planes de seguridad de TI tiene implementados en el bufete?	Dpto. TI Directiva de Negocio
¿Qué medios emplean para comunicar las medidas de seguridad a los empleados?	Dpto. TI

¿Quién tiene acceso a las dependencias con infraestructura TI sensible del despacho	Directiva de Negocio
¿Los usuarios desplazados en cliente disponen de algún método de encriptación cuando están conectados a la red del cliente?	Dpto. TI
¿Qué tipo de filtro se está aplicando al acceso a la red inalámbrica del despacho?	Dpto. TI
¿Es posible acceder a los servidores mediante la red inalámbrica para visitas?	Dpto. TI
¿Se tienen identificados los casos de riesgo de seguridad de TI y su consecuente actuación?	Dpto. TI Usuarios
¿Existe un protocolo de revocación de claves de acceso a los empleados despedidos o que dimiten?	Dpto. TI

Tabla 39 - Cuestionario DS5

Métricas a analizar:

- # de puestos sin contraseña de bloqueo
- Tiempo que transcurre entre que el usuario abandona su puesto y se bloquea su equipo
- # de veces que se deja abierta la puerta del cuarto de servidor
- # de accesos incontrolados a dependencias sensibles del despacho (sala de fax, sala de servidor, sala de escáner)
- Frecuencia con la que se cambian las contraseñas de los equipos
- Rango de alcance de la red inalámbrica para visitas
- Tiempo transcurrido entre una falla de seguridad TI y su conocimiento por parte del responsable de seguridad TI.

Proceso DS7

Como sucede con cualquier herramienta de trabajo, es necesario que el usuario conozca cómo funciona y cómo manejar los dispositivos TI que están a su alcance para lograr sus objetivos en el bufete. Es

importante que el usuario reciba una correcta formación sobre sus instrumentos de trabajo para realizar sus tareas de manera eficaz, eficiente y segura.

En el ámbito del bufete, la mayoría de abogados conocen la suite ofimática *Office* que utilizan para prácticamente todas sus operaciones (escritos, gestión de correos) y eso es algo común en la mayoría de los despachos. Sin embargo, cada despacho tiene su propio sistema de organización documental, su propio aplicativo de imputaciones de gastos y minutas, sus propios accesos a las unidades de red y servicios compartidos y para terminar, el manejo de aparatos como son el escáner, o el fax.

Respecto a estos últimos dispositivos, en ocasiones el abogado delega en las secretarias del bufete para realizar estas tareas administrativas. Pero ocurre que por cuestiones de disponibilidad, incompatibilidades de horario o simplemente, por privacidad de los datos a tratar, es el propio abogado quien tiene que realizar dichas tareas. Por este motivo, es interesante que todos los miembros del bufete sepan manejar el 100% de la infraestructura TI, dentro del marco de su trabajo y nivel de seguridad.

Cuestionario:

Cuestión	Persona implicada
¿Cómo se realizan los grupos objetivo para recibir la formación?	Directiva de negocio Dpto. TI
¿Qué canales se emplean para impartir la formación?	Directiva de negocio
¿Poseen comunicación con la gerencia para indicar las necesidades formativas?	Usuarios finales Dpto. TI
¿Se realiza algún tipo de seguimiento del proceso de formación?	Directiva de negocio
¿Se tienen en cuenta las opiniones sobre la formación recibida?	Usuario final

Tabla 40 - Cuestionario DS7

Métricas para analizar los objetivos de control:

- Tiempo que tarda el empleado recién incorporado en recibir su formación.

- # de consultas realizadas por el empleado sobre manejo de sistemas TI.
- # de errores cometidos por usuarios que han recibido formación.
- # de cuestiones realizadas posteriormente sobre puntos relativos a la formación recibida.
- # de cuestiones recibidas por el Dpto. TI que no están incluidas en la documentación de la formación.
- # de fallos relativos al manejo de los aplicativos.
- Mejora en la productividad
- Tiempo empleado en ejecutar aquellas tareas que dependan de TI
- Recursos (humanos, financieros) empleados en las labores de enseñanza
- Calificación posterior del usuario sobre la formación recibida

Proceso DS8

Uno de los principales cometidos del Dpto. TI en un bufete es la resolución de incidencias. En este caso, una buena gestión del soporte técnico, tanto para quien lo solicita como para quien lo recibe, se basa en la correcta administración de la mesa de servicio. Los abogados contactan directamente con el correo de contacto del dpto. TI destinado a las incidencias y en función de la urgencia de las peticiones en caso de que ocurran varias a la vez, el responsable atiende la más crítica.

En caso de que varios incidentes se repitan o tengan un origen o causa común, es competencia del empleado de TI determinar cuál puede ser el problema que cause estas incidencias y tomar las medidas correspondientes. En algunos casos, la solución puede estar en sus manos, en el caso de que un enrutador tenga un funcionamiento errático y afecte un grupo de usuarios, puede revisar las conexiones. Pero si se trata de un problema que escapa a sus manos, deberá ponerse en contacto con la gerencia para determinar qué medidas tomar.

En el caso de que el Dpto. TI esté compuesto por una única persona como fue mi caso, el proceso de escalado es un poco distinto al que puede ser habitual en bufetes de mayor envergadura. En ese caso, se puede recurrir a los proveedores de servicios o a la búsqueda de información en internet cuando se trata de incidencias que pueden ser generales y no específicas de la infraestructura TIC de la empresa.

Cuestionario:

Cuestión	Persona implicada
¿Se involucra la gerencia en la toma de decisiones para la resolución de problemas?	Directiva de negocio Dpto. TI
¿Existe alguna estructura organizacional en la empresa destinada a la gestión de incidentes y problemas?	Directiva de negocio Dpto. TI
¿De qué manera contactan los usuarios con el Dpto. TI?	Usuarios finales
¿Existe un protocolo de escalado de incidencias según su criticidad?	Dpto. TI
¿Los empleados del dpto. TI reciben la formación adecuada cuando se adquieren nuevos recursos de TI?	Dpto. TI Directiva de negocio
¿Existe algún aplicativo para la gestión de incidencias?	Dpto. TI

Tabla 41 - Cuestionario DS8

Métrica a analizar:

- # de incidencias sin actualizar su estado.
- # de incidencias escaladas.
- # de incidencias reabiertas
- # de incidencias documentadas.
- # de incidencias resueltas en remoto
- Duración de las llamadas telefónicas.
- Tiempo de respuesta a la petición del usuario.
- Frecuencia con la que se repiten las mismas incidencias
- Grado de satisfacción del usuario

Proceso DS11

Un ordenador estropeado puede arreglarse o sustituirse; si la red se cae, se puede recurrir a otro proveedor de respaldo; en general, una incidencia o problema en la parte física de la infraestructura de TIC de una empresa tiene, o suele tener, solución. Sin embargo, toda la capacidad operacional de TI se viene abajo si fallan o faltan los datos, la información. Y dentro de un bufete, los datos son un componente muy importante y delicado para su operativa. La aplicación de este proceso es crucial para asegurar la integridad, la disponibilidad y la protección de los datos que maneja un bufete. En caso contrario, redundaría en un perjuicio moral y económico grave para el bufete.

En un bufete, los datos pueden clasificarse según su origen, destino y sensibilidad de su contenido, dando lugar a su clasificación por niveles de seguridad. Como se ve en la gráfica, el bufete está en contacto con las administraciones públicas y sus clientes. Estos tienen varias formas de ponerse en contacto con el bufete según las necesidades y el tipo de información transmitida:

- Fax: burofax, contactos con otros despachos o empresas
- Correo ordinario: cartas certificadas, avisos, notificaciones
- Correo electrónico: escritos, alegaciones, consultas con clientes o administraciones.

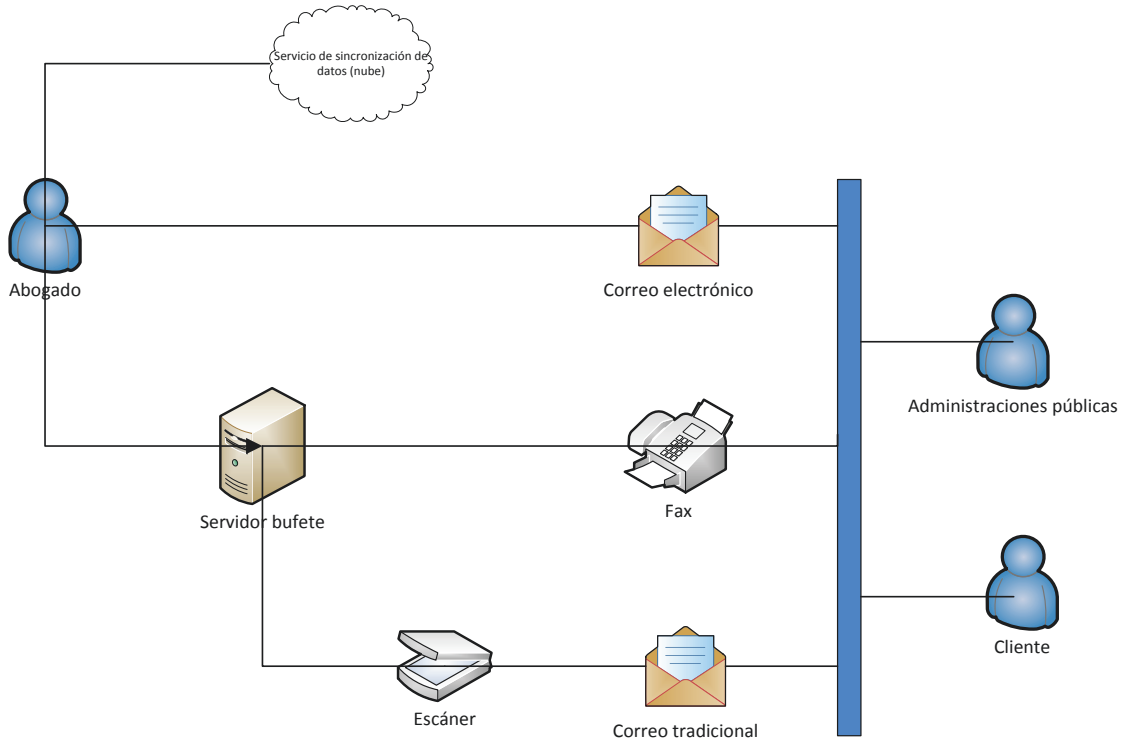


Figura 11 - Flujo de datos en el despacho

Para asegurar que los procesos anteriormente mencionados se cumplen, a continuación figuran un cuestionario y unas métricas a analizar por parte del auditor.

Cuestionario:

Cuestión	Persona implicada
¿Existe un plan estratégico de gestión de los dispositivos de almacenaje?	Directiva de negocio
¿Existe una jerarquía de usuarios que determine a qué ficheros pueden acceder?	Directiva de negocio
¿De qué forma se asegura el acceso físico a los servidores?	Dpto. TI
¿Los dispositivos personales de almacenamiento de datos disponen de clave de seguridad?	Dpto. TI

¿Existen cláusulas de confidencialidad para empleados?	Directiva de negocio
¿Los proveedores de servicios han firmado acuerdos de confidencialidad?	Directiva de negocio
¿Qué tipo de cifrado tienen las claves de acceso al servicio de almacenamiento en la nube?	Dpto. TI
¿El acceso a las carpetas compartidas del servidor está protegido?	Dpto. TI
¿Con qué frecuencia se renuevan las claves de acceso al servicio de almacenamiento en la nube?	Dpto. TI
¿Los archivos adjuntos a los correos tienen algún tipo de encriptado?	Usuarios finales Dpto. TI
¿Los equipos disponen de software antivirus actualizados?	Dpto. TI
¿Se establecen políticas de usuario "administrador" en los portátiles de los usuarios?	Dpto. TI
¿Los correos electrónicos disponen de firma electrónica para el contacto con clientes?	Dpto. TI
¿Los correos electrónicos de los abogados vienen dotados de *disclaimer*?	Usuarios

Tabla 42 - Cuestionario DS11

Con "Documento de seguridad" se hace referencia a un documento en el cual figuran todas las medidas de seguridad, técnicas y organizativas, que garantizan la seguridad de los datos. Las medidas de seguridad varían en función de los datos tratados por el bufete.

Dentro del bufete, existen algunos puestos de trabajo cuyas tareas requieren la manipulación de multitud de documentos y de información de toda naturaleza y sensibilidad, ya sea recibiendo documentos por correo ordinario que tienen que escanear, recepción de faxes para clasificar, soporte técnico a usuarios, accesos a los servidores. Es importante que existan distintos formatos de cláusulas de confidencialidad en función de estos perfiles.

Métricas:

- # de fallos de acceso a un documento.
- # de documentación sensible mal archivada.
- Fecha de revisión del documento de seguridad.
- # de datos no actualizados.
- # de ficheros no encontrados en su ubicación original.
- # de ficheros irrecuperables.
- # de ficheros mal borrados.
- # de ficheros recuperados con éxito.
- # de correos enviados sin las medidas de seguridad oportunas.
- # de portátiles con el software antivirus desactivado.
- % de pérdida en el negocio por pérdida/inconsistencia de datos.
- # de reclamaciones por parte de los clientes.
- # de correos electrónicos no recibidos por el cliente.
- # de correos electrónicos recibidos con código malicioso detectado.

Proceso DS12

Este proceso tiene como fin evaluar las medidas de seguridad adoptadas por la organización con respecto a la infraestructura física de sus instalaciones. El concepto de ambiente físico no se queda únicamente en la infraestructura TI, sino que atañe también al propio negocio y al emplazamiento en donde los usuarios realizan sus labores. La protección de los elementos físicos de la infraestructura TI del negocio va desde la defensa frente a ataques externos hasta los descuidos de los propios usuarios.

En este punto, el auditor analizará los puntos relativos a la protección física de los elementos anteriormente descritos mediante el siguiente formulario y el análisis de las métricas.

Cuestionario:

Cuestión	Persona implicada
¿Se han tenido en cuenta las normas de seguridad física y leyes de seguridad y salud en el trabajo para definir y diseñar las ubicaciones de los equipos TI?	Directiva de negocio
¿Las medidas de seguridad se han definido de modo que queden alineadas con los requisitos de negocio?	Directiva de negocio Dpto. TI
¿Se han diseñado e implementado medidas de protecciones medioambientales para los servidores de las oficinas?	Directiva de negocio Dpto. TI
¿Se ha definido un protocolo para revocar el acceso a las dependencias de los recursos TI a los empleados despedidos?	Dpto. TI
¿Se realizan pruebas de simulacros de incendio?	Directiva de negocio
¿Los responsables del control de acceso a las dependencias de las oficinas saben cómo proceder en caso de acceso no permitido?	Directiva de negocio
¿El cableado Ethernet del bufete está protegido?	Dpto. TI
¿Se realiza el borrado completo de los datos cuando se entrega un equipo a reparación o sustitución?	Dpto. TI
¿Reciben los usuarios formación de concienciación de la seguridad TI?	Usuarios
¿Las mesas se mantienen libres de cualquier elemento pernicioso para los periféricos?	Usuarios

Tabla 43 - Cuestionario DS12

Métricas:

- # de empleados que han rellenado el cuestionario de prevención de riesgos laborales
- # de apagados forzados del servidor
- # de veces que la sala de servidor queda abierta

- # de incidencias de los periféricos de la oficina
- Tiempo que el negocio queda suspendido por incidentes ambientales
- # de elementos TI retirados del despacho sin permiso ni autorización
- # de conexiones eléctricas susceptibles de malfuncionamiento

Proceso DS13

El análisis y supervisión de la gestión de procesos también tiene su importancia en un negocio como la abogacía. El equipo o el profesional encargado de la supervisión de los procesos TI que dan soporte al negocio han de realizar su labor de forma eficiente para el negocio. Esto es, realizar sus labores de forma que interfieran lo menos posible en el trabajo de los abogados.

Por otra parte, aquellos procesos de actualización de aplicaciones o salvaguarda/sincronización automática de datos han de realizarse en sintonía con las tareas que desempeñan los abogados. Un ejemplo de esta planificación sería la definición de horarios valle en los cuales el uso de recursos TI sea el mínimo, para permitir la ejecución de estas tareas de mantenimiento.

Mediante el siguiente cuestionario y las posteriores métricas, el equipo auditor se podrá determinar el nivel de madurez de este proceso.

Cuestionario:

Cuestión	Persona implicada
¿Se implementan procedimientos de mantenimiento preventivo de SW y HW?	Dpto. TI
¿Se alinean las prioridades de negocio con las necesidades de los procesos de mantenimiento?	Dpto. TI
¿Se tienen en cuenta los términos de confidencialidad, integridad y disponibilidad de los datos?	Dpto. TI
¿Se entregan los servicios TI en los términos que estipula el plan estratégico de TI definido?	Directiva de negocio Usuarios finales
¿Se analizan las cargas de trabajo del bufete para planear los procesos de actualización/sincronización?	Dpto. TI

¿Se actualiza la documentación de formación en función de las nuevas funcionalidades derivadas de las actualizaciones?	Dpto. TI
¿Se actualizan los procesos de mantenimiento/actualización en función de las necesidades del negocio?	Dpto. TI
¿Existe un documento de resguardo de la información crítica?	Dpto. TI
¿Existe un plan de clasificación y almacenamiento de información según su criticidad y sensibilidad?	Usuarios Dpto. TI
¿Existe comunicación entre usuarios y Dpto. TI para avisar de paradas de servicio o procesos de actualización/mantenimiento de urgencia?	Usuarios Dpto. TI

Tabla 44 - Cuestionario DS13

Métricas:

- % de aplicaciones incluidas en los procesos de actualización automática.
- % de infraestructura TI incluida en el mantenimiento previo.
- # de datos inaccesibles durante un proceso de actualización de aplicación.
- # de incidencias derivadas de actualizaciones de aplicaciones
- Tiempo de inactividad de los usuarios.
- Frecuencia de actualización de planes de mantenimiento.
- # de problemas derivados por falta de mantenimiento de recursos TI.
- # de dispositivos de almacenamiento de datos incorrectamente desechados
- % de la relación con empresas de paquetería cubierta con acuerdos de confidencialidad y seguridad.
- # de interrupciones de servicios TI sin previo aviso

Proceso ME1

Es importante definir un marco de trabajo en el cual se pueda monitorear y evaluar el correcto desempeño de los recursos TI que prestan servicio a los abogados. Este marco de trabajo consistiría en determinar una serie de objetivos de desempeño fácilmente medible por los usuarios del dpto. TI de modo que pueda ser corregido a posteriori para mejorar la usabilidad TI. Se establece un lapso de tiempo en el cual se evalúan y califican ciertos aspectos medibles de los recursos TI.

Es importante detectar los riesgos a los que se enfrenta la implantación y el funcionamiento de los recursos TI en un bufete. La detección prematura de estos riesgos permite evitar futuros problemas en el marco de las TIC del bufete.

Mediante el siguiente cuestionario y el análisis de las métricas, el equipo auditor podrá determinar si se cumplen correctamente los objetivos de control destinados a este propósito. Y a continuación, serán capaces de poder emitir las pertinentes recomendaciones.

Cuestionario:

Cuestión	Persona implicada
¿Se realizan revisiones a las TI de forma regular?	Directiva de negocio
¿Cómo se siente conforme a las TIC del bufete?	Directiva de negocio Usuarios
¿La empresa dispone de un plan de actualización de las TI?	Directiva de negocio
¿Se documentan los procesos de actualización/mejora de las TI del bufete?	Dpto. TI
¿El Dpto. TI está correctamente alineado con los demás departamentos?	Directiva de negocio
¿Los usuarios son conscientes de los objetivos y metas de las TI en el negocio?	Usuarios Directiva de negocio

Tabla 45 - Cuestionario ME1

Métricas:

- # de personas encargas de revisar los recursos TI
- Balance entre inversión TI y beneficio reportado al bufete
- # de riesgos detectados
- Tiempo que se tarda en identificar un problema derivado de varios riesgos
- % de objetivos de desempeño alcanzados
- # de quejas recibidas por los usuarios respecto a TI

Proceso ME3

Existe una paradoja a la hora de evaluar este proceso en relación al artículo 7.5 de LOPD. Este artículo determina la prohibición de tratar documentos relativos a la comisión de infracciones penales o administrativas, especificando que este tipo de dato sólo puede estar incluido en los ficheros de las Administraciones públicas. Sin embargo el bufete necesita tratar estos datos para proteger y preparar la defensa de su cliente, por lo tanto acaba por establecerse un juicio de proporcionalidad en el que prima el servicio del bufete con respecto a su cliente frente a lo que estipulan algunos artículos y leyes de protección de datos.

Otro aspecto a controlar en lo relativo al control regulatorio es la administración de aplicaciones y la piratería. Dado el reducido tamaño del bufete, los usuarios pueden verse tentados de usar software de licencia no comercial o incluso software pirata. Esto puede redundar en numerosos problemas, además de los obvios legales. Un programa de procedencia no segura puede contener software malicioso que puede perjudicar los recursos del bufete. Al no disponer de una licencia de uso, el bufete pierde las mejoras derivadas de las constantes actualizaciones que liberan las empresas desarrolladoras, carecen del soporte técnico de éstas a sus clientes.

Cuestionario:

Cuestión	Persona implicada
¿Existe un plan de definición de niveles de seguridad para los datos gestionados en el bufete?	Directiva de negocio

¿Se realizan correctamente la inscripción de ficheros de datos sensibles en la Agencia Española de Protección de Datos (AEPD)?[*aepd*]	Directiva de negocio
¿Con qué frecuencia se hace la revisión del cumplimiento regulatorio?	Directiva de negocio
¿Los clientes disponen de los medios para ejercitar su derecho de acceso, rectificación y cancelación de datos?	Directiva de negocio Dpto. TI
¿Se emplean aplicaciones con licencias de uso no comercial o privado?	Usuarios
¿Se conservan las pruebas y evidencias de adquisición y propiedad de licencias de aplicaciones?	Dpto. TI
¿Existe un catálogo con los tipos de archivos manejados en el bufete relacionados con su correspondiente nivel de seguridad?	Directiva de negocio
¿La información que maneja el bufete sobre sus clientes ha sido recabada con consentimiento expreso y por escrito por estos?	Directiva de negocio
¿Se verifica que los proveedores externos de servicios cumplen con la normativa regulatoria correspondiente?	Directiva de negocio
¿El servicio de sincronización de datos cumple la normativa española de protección de datos personales?	Directiva de negocio
¿El enlace al texto de "*Aviso legal*" en la web es visible y fácilmente localizable por el visitante?	Directiva de negocio
¿Tiene destructora de papel para desechar documentación sensible?	Usuarios
¿Los usuarios están sensibilizados con las medidas a tomar para la Protección de Datos?	Directiva de negocio Usuarios
¿Está presente en los correos a los clientes la referencia a la LOPD en la firma del abogado?	Usuarios

Tabla 46 - Cuestionario ME3

La relación que tiene el bufete con la empresa *SugarSync* es únicamente de almacenaje y sincronización de datos. Por ello debe analizar si dicha empresa cumple la normativa española de protección de datos. Y por otra parte se debe garantizar que cumple la normativa con respecto al movimiento internacional de datos. Se verificará que la empresa proporcione un nivel de protección equiparable al que presta la LOPD.

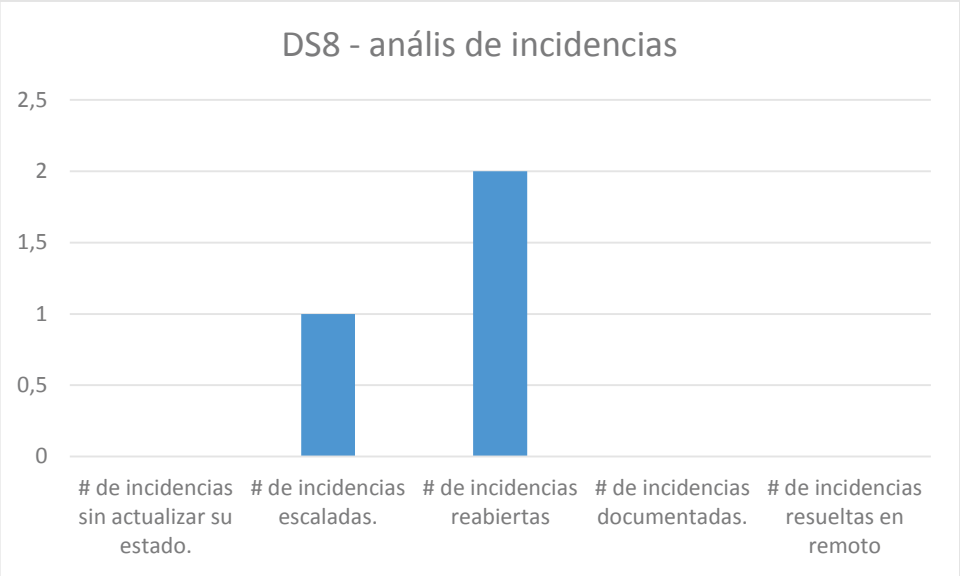
Métricas a analizar:

- # de software ilícito detectado en los dispositivos TI destinados al negocio.
- # de aplicaciones que se emplean sin su correspondiente activación.
- % de datos sensibles del bufete adscritos a la AEPD.
- # de clientes que no han podido ejercer sus derechos de modificación de datos.
- # de usos no autorizados de los recursos de procesamiento de datos.
- # de ficheros de datos cuya clasificación no corresponde a su nivel de seguridad determinado por la LOPD.
- # de correos enviados sin firma de privacidad de datos

Gráficas de análisis

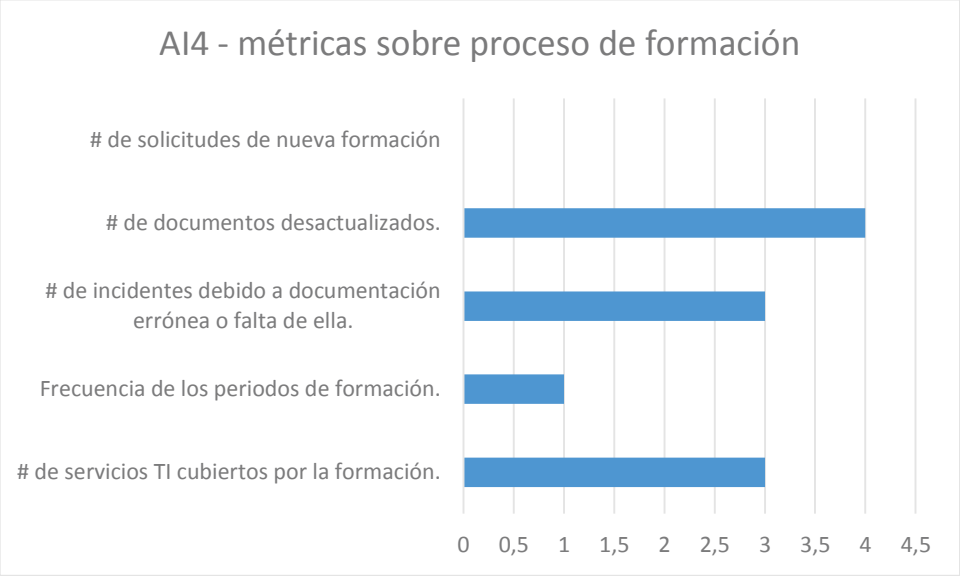
Mediante el uso de una tabla Excel, se pueden analizar los valores de las distintas métricas empleadas para cuantificar el desempeño de los procesos. Mediante la configuración de las celdas y los valores que se presentan, puede ser todo lo potente que necesite el equipo auditor. Se presentan las cuestiones conectadas con el destinario y su respuesta. Y por otra parte, las métricas con sus valoraciones, las cuales pueden usarse para construir las gráficas de análisis. A modo de ejemplo, procedo a presentar algunos ejemplos. Se han usado unos valores arbitrarios para conformar las gráficas y dar una idea de cómo aparecería el resultado real.

Gráfica de las métricas relacionadas con las incidencias del proceso DS8. Los valores de cada color pueden consultarse en la hoja Excel adjunta a la memoria.



Gráfica 1 - Métricas de DS8

Otro ejemplo con una presentación distinta es la relativa al proceso AI4:



Gráfica 2 - Métricas de AI4

Añado un acceso directo al archivo Excel para su posterior consulta:

PFC - definición marco trabajo COBIT

Universidad Carlos III de Madrid

Definición de un marco de trabajo basado en CObIT para la auditoría TI de un bufete

Planear y Organizar

Entregar y Dar Soporte

Adquisición e Implantación

Monitorear y Evaluar

Lista de valores

Gráficas de análisis

5.- Gestión del Proyecto

Este capítulo del proyecto consiste en la exposición de los pasos que se han realizado para la aplicación real del proyecto. Se mostrarán de forma detallada los pasos a realizar y se presentarán mediante un diagrama de Gantt, acompañado de un resumen de los costes necesarios para su puesta en marcha real.

Gestión del proyecto

El proyecto se ha estructurado en función de las siguientes fases:

1. Estudio de metodologías: quizá la más importante, debido a la variedad de metodologías de Gobierno de TI que existen en el mercado. Durante esta fase analicé y estudié el contenido y el enfoque de las técnicas de gobierno TI más importantes para tratar de encontrar la que más se adaptaba a lo que quería hacer como proyecto.
2. Análisis del bufete: esta fase se podría dividir en dos subgrupos debido a la naturaleza del análisis y la información que se va a necesitar para la siguiente etapa.
   2.1. Entrevistas: Se realizan una serie de entrevistas y charlas preliminares con los miembros del bufete de modo que se pueda analizar las necesidades del bufete en cuanto al uso de las TIC.
   2.2. Análisis TI: análisis de los recursos TI presentes en el bufete y del uso que se hace de ellos.
3. Selección de procesos CObIT: En función de los datos recogidos en la fase anterior, he seleccionado los procesos CObIT que he considerado como aptos para este proyecto y he realizado una descripción/explicación de cómo se aplican al negocio.
4. Base de análisis y control: Tras la decisión de los procesos que se van a aplicar, hay que analizar cada uno de ellos para determinar qué objetivos de control y métricas son las adecuadas para configurar un buen plan de auditoría informática.
5. Validación del proyecto
   5.1. Revisión final del tutor: esta fase ha consistido en un intercambio de correos en los cuales el tutor ha sugerido una serie de modificaciones para que la memoria fuese apta para su entrega al tribunal.
   5.2. Preparación de la defensa: durante este tiempo se ha preparado la presentación en formato PPT para su defensa frente al tribunal de la UC3M.
6. Realización de la documentación: esta tarea tiene su inicio el primer día que empiezo con este proyecto y finaliza tras aplicar las últimas recomendaciones de mi tutora. Engloba el resto de tareas,

es la única que se ejecuta de forma "paralela" al resto de proyectos, puesto que durante toda la vida del proyecto, se han incluido datos de investigación, resultados obtenidos de las entrevistas con los empleados, etc.

La primera tarea que he incluido en el esquema referente a la definición del proyecto se refiere al tiempo que se ha empleado en buscar un tema sobre el cual realizar el proyecto.

La ejecución del proyecto ha sido realizada por una única persona, por lo que ciertas fases del proyecto han sido escalonadas y no han podido coincidir en el tiempo, a excepción del proceso de documentación, que se ha realizado de forma "paralela" según avanzaba cada fase.

Diagrama de Gantt

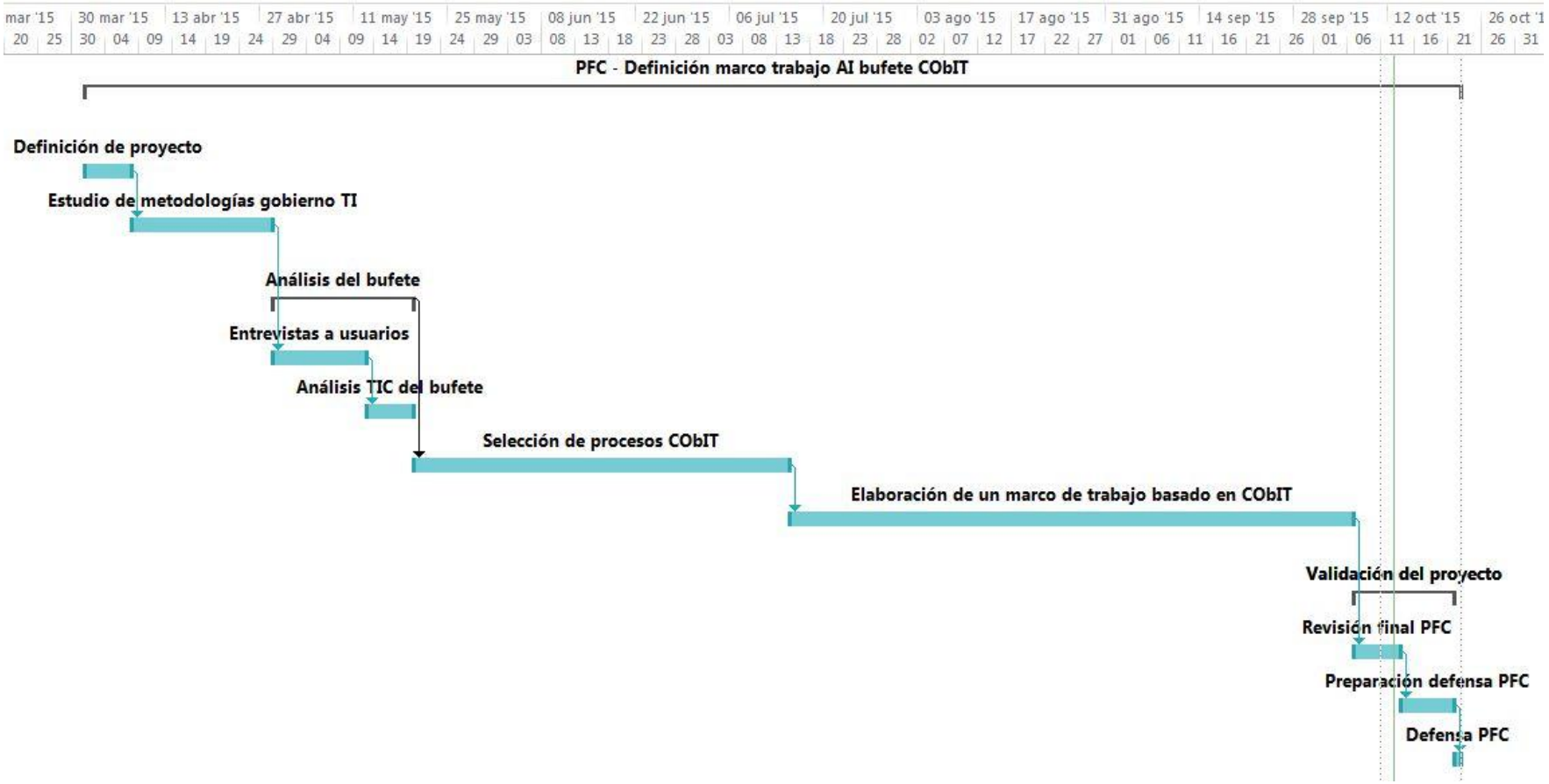


Figura 12 - Diagrama de Gantt

A continuación presento el calendario en detalle del desarrollo del proyecto:

	Nombre de tarea	Duración	Comienzo	Fin	Prec
1	**PFC - Definición marco trabajo AI bufete CObIT**	**147 días**	**mié 01/04/15**	**jue 22/10/15**	
2	Definición de proyecto	5 días	mié 01/04/15	mar 07/04/15	
3	Estudio de metodologías gobierno TI	15 días	mié 08/04/15	mar 28/04/15	2
4	Análisis del bufete	15 días	mié 29/04/15	mar 19/05/15	
5	Entrevistas a usuarios	10 días	mié 29/04/15	mar 12/05/15	3
6	Análisis TIC del bufete	5 días	mié 13/05/15	mar 19/05/15	5
7	Selección de procesos CObIT	40 días	mié 20/05/15	mar 14/07/15	4
8	Elaboración de un marco de trabajo basado en CObIT	60 días	mié 15/07/15	mar 06/10/15	7
9	Validación del proyecto	11 días	mié 07/10/15	mié 21/10/15	
10	Revisión final PFC	5 días	mié 07/10/15	mar 13/10/15	8
11	Preparación defensa PFC	6 días	mié 14/10/15	mié 21/10/15	10
12	Defensa PFC	1 día	jue 22/10/15	jue 22/10/15	11

Tabla 47 - Calendario del proyecto

Análisis de costes

En este punto se presentan los costes que ha incurrido la realización de este proyecto, tanto en recursos humanos como en recursos TI.

El desarrollo del proyecto ha sido realizado por un ingeniero informático de perfil analista y durante ciertas etapas del proyecto, ha sido necesaria la consulta a un abogado consultor para tratar ciertas etapas del análisis legislativo bajo el cual opera el bufete. Estas horas de trabajo y el personal necesario para el desarrollo de este proyecto se detalla en la siguiente tabla:

Rol	horas trabajadas / semana	coste / hora (€)	Coste total (27 semanas)
Ingeniero analista	40	25	27000
Abogado consultor	5	30	4050
Total			31050

Tabla 48 - Coste personal

Durante la realización del proyecto se ha incurrido en otros costes en elementos materiales o logísticos:

- Gastos hardware: se ha empleado un ordenador portátil durante todo el proyecto, así como una impresora y dispositivos de almacenaje.
- Viajes: durante la etapa del análisis del bufete, se han realizado viajes a las oficinas para entrevistarse con los usuarios y analizar el entorno de uso de las TIC.
- Material de oficina: bolígrafos, cuadernos, fotocopias

Descripción	Coste	% dedicación PFC	Dedicación (meses)	periodo de depreciación	Coste Imputable
Portátil Compaq Presario CQ62	550	100	6,75	60	61,875
Impresora Epson multif	80	100	1	60	1,333333333
USB stick 32GB	25	100	6,75	60	2,8125
Total					232,03125

Tabla 49 - Gastos SI

Fórmula empleada para el cálculo de la amortización:

$\frac{A}{B} * C * D$ Siendo

A	nº de meses desde la fecha de facturación en que se utiliza el equipo
B	Periodo de depreciación
C	Coste del equipo (sin IVA)
D	% del uso que se dedica al proyecto

El gasto relativo al software empleado en el desarrollo del proyecto no es imputable al coste total ya que la licencia ya venía incluida en el equipo cuando se adquirió.

Finalmente, así queda representado el coste total del proyecto:

Descripción	coste
Recursos humanos	31050
Recursos SI	232,03
Viajes (visitas bufete, reuniones con abogado consultor)	60
Gastos varios (papelería, reuniones con consultor, imprevistos)	50
Total gastos	31392,03
Prima por riesgo (15%)	4708,8
Total (riesgo inc)	36100,83
Beneficio (20%)	7220,166
Base imponible	43320,996
I.V.A (21%)	9097,40916
Total (IVA inc)	**52418,40516**

Tabla 50 - Presupuesto final PFC

6.- Conclusiones y líneas futuras

Conclusiones

El desarrollo de este proyecto me ha permitido ampliar mis conocimientos del mundo de la pequeña y mediana empresa, sus riesgos, los objetivos, la manera de trabajar y cómo se organiza un bufete internamente. Y una de sus principales dificultades que es la competencia. Al nivel de las grandes empresas y compañías, la competencia es menos numerosa, pero al nivel en el que opera este tipo de bufetes, son más numerosos los competidores que ofrecen servicios similares. No disponen de una gran fama que les sirva de tarjeta de visita como *Cuatrecasas, Garrigues* o *Uría* y han de recurrir a su buen hacer, tarifas y dedicación al cliente. Y es precisamente debido a esa competencia que estas pequeñas y medianas firmas no pueden permitirse flojear en aspectos que no sean los propios de su negocio.

Durante la elaboración de este proyecto, he podido mejorar y ampliar los conocimientos que tenía sobre la auditoría informática y el gobierno de TI, algunos de los temas que más me llamó la atención referente a mi formación académica. Aunque el primero de estos no es tema principal de mi proyecto, el producto de éste sí está orientado a que un auditor tenga una buena base para realizar su trabajo. Además, he adquirido conocimientos sobre metodologías, técnicas y métodos de gobierno de TI. Lo que me ha mostrado la gran evolución que han tenido estas técnicas. Siendo esto un reflejo del aumento de la importancia que tienen los datos y la información en la buena consecución del negocio. Pero igual de importante es la correcta administración de estos activos, como el buen uso que se hace de los elementos físicos de las TI.

La elección de CObIT y su manejo pueden parecer simples a primera vista, sin dificultades técnicas como podría ser la definición y desarrollo de una aplicación. Respecto a la primera dificultad, he tenido que analizar y comparar varias herramientas de control y gobierno de TI, analizar sus pros y sus contras, estudiar si eran aplicables a este bufete y si me iban a proporcionar el resultado que yo deseaba. En cuanto al manejo de CObIT, me he encontrado con el principal problema que ha sido el determinar correctamente qué procesos tenían sentido para aplicar a este bufete o uno de similares características. Habría sido más fácil seleccionar y poner en práctica todos los procesos para definir el marco de trabajo para una futura auditoría pero creo que, seleccionando los procesos que realmente tienen sentido, he logrado definir una base para una AI más eficiente y hecha a medida para un bufete de estas dimensiones.

Líneas futuras

Tras el desarrollo de este proyecto, surgen tres líneas futuras de manera inmediata:

- El desarrollo de una aplicación que permitiese a un auditor ejecutar esta guía sobre cualquier bufete. En función de los valores introducidos en el formulario automatizado, se generarían una serie de resultados cuantificables que podrían ser aplicados para determinar la madurez en términos de TI del bufete. Tras la finalización de la auditoría, el equipo de especialistas entregará a la dirección de la gerencia los resultados obtenidos. En base a estos resultados, el equipo auditor podrá emitir una serie de recomendaciones para la mejora en el ámbito de las TIC dentro del bufete.
- Puesto que todo es mejorable en este mundo, y aún más en las TIC, la evolución de Cobit 4.1 a Cobit 5 sería otro proyecto a tener en cuenta. Ha pasado un cierto tiempo desde que inicié este proyecto basado en Cobit 4.1 y durante éste, la fundación que compone ISACA ha evolucionado la metodología Cobit hasta la actual versión 5, más enfocada al negocio.
- Como tercera vía de aplicación cabe la posibilidad de obtener una certificación ISO de calidad especialmente destinada al gobierno de TIC: UNE-ISO/IEC 20000 [*iso20000*] o una norma adaptada y enfocada a la gestión de TIC en un bufete. Cada empresa o tipo de negocio tiene su particularidad y no sería justo englobar a bufetes, estudios de arquitectura o empresas de reparto bajo el mismo paraguas normativo. No es suficiente la realización de una auditoría de sistemas para lograr una ISO, son necesarios varios pasos más, pero es un punto importante en el camino hasta lograr una certificación de calidad. De esta forma, el negocio lograría un reconocimiento extra además de posicionarse por encima de la competencia.

Estos tres puntos son los iniciales y quizá, los más obvios tras la lectura de este proyecto. Pero tras la realización del proyecto y el análisis de los procesos de auditoría, de la variedad de perfiles de auditores informáticos que puede haber y las necesidades de conocimientos que abarcan desde lo legislativo hasta los tecnicismos de las TIC, me surge una idea para una posible ampliación de este proyecto, o incluso para la realización de uno nuevo.

Consistiría en la definición de una propuesta para un plan de estudios especializado en la auditoría informática a PyME's. Enfocado a un mundo empresarial que depende mucho de las TIC, pero que no

realizan grandes desarrollos TI, por lo que la formación técnica a nivel de desarrollo técnico, ciclo de vida de software no deberá ser muy alta. Pero sí en lo relativo a la gestión de redes y gestión y administración de aplicativos y bases de datos, que deberá ser extensa puesto que una de las bases de la buena consecución del negocio es la posibilidad de comunicarse con sus clientes y entre empleados.

Como hemos visto en el desarrollo del proyecto, el bufete tenía ciertas aplicaciones desarrolladas a medida para sus necesidades, pero el porcentaje de este tipo de aplicativo en una PyME no suele superar el 15/20% mientras que el resto de aplicaciones que emplean son aplicaciones adquiridas con un desarrollo prestablecido, para el gran público. En ocasiones, los conocimientos que pueden encontrarse navegando por internet acerca de cómo manejar estas aplicaciones no son suficientes, y por eso sería otro aspecto fundamental en el plan formativo de este plan de estudios.

Del apartado técnico pasaríamos al apartado enfocado al negocio y la gestión empresarial. Una de las mayores dificultades que he tenido a la hora de desarrollar este proyecto es el aspecto legal del negocio y de la operativa del bufete. Es importante para aquellos que vayan a enfrentarse a un proyecto de tal calibre, el tener una buena base de conocimiento empresarial para saber cómo funciona una empresa, cuáles son sus posibles riesgos, saber entender rápidamente su visión y su misión y de qué forma pueden las TIC ser un componente más de cara a la consecución de sus objetivos.

ANEXOS

Anexo I: L.O.P.D.

Este anexo contiene parte de la L.O.P.D. con los artículos que he estimado oportunos nombrar y utilizar en la realización de esta auditoría, teniendo en cuenta el tipo de empresa que se está evaluando. Son los artículos y regulaciones que se deberán de auditar en el proceso ME3 para evaluar el cumplimiento regulatorio.

1.- Política de privacidad

El artículo 5 de LOPD rige el comportamiento de cualquier empresa con respecto al manejo y tratamiento de datos personales de usuarios o clientes. Dos claros ejemplos en el bufete son el formulario de contacto para potenciales clientes y el canal de comunicación para el envío de CV de los candidatos.

Artículo 5. Derecho de información en la recogida de datos.

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Siguiendo con la gestión de datos privados y la gestión por parte del bufete, el artículo 6 especifica la forma en la que el bufete puede recabar la información personal de clientes y usuarios:

Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

2.- Calidad de los datos

Los datos recogidos por el bufete de sus clientes o de otros socios deben responder a los criterios de exactitud, suficiencia y necesidad. Solo se obtendrá la información necesaria para el correcto desempeño de la labor del bufete y no se añadirán más datos de los estrictamente necesarios. Serán exactos y puestos al día de forma periódica de acuerdo a la situación actual del cliente. Cuando la relación del bufete con su cliente o un socio finalice, estos datos serán cancelados. Todo esto viene explicado y detallado en el artículo 4:

Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

3.- Deber de secreto

Los responsables del Fichero y todos aquellos abogados que trabajen con la información de clientes están obligados a mantener el secreto profesional. En un bufete es muy habitual que un caso sea tratado por un equipo de varias personas, o que los responsables de la recepción de la oficina manejen información de carácter sensible por lo que es importante velar por el cumplimiento de estas normas. Este punto queda reflejado en el artículo 10:

Artículo 10. Deber de secreto.

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

4.- Cesión y transferencia de datos

Tanto por la operativa del bufete como por su gestión interna, el manejo de información personal que se realiza ha de estar supeditado a varios artículos de la LOPD. El departamento de RRHH transmite y almacena información de los empleados para la gestión de nóminas, en conjunción con una gestoría. Por otra parte, el bufete tiene un contrato con una empresa de almacenamiento online en donde guarda sus ficheros. Las medidas de seguridad que se han de aplicar aparecen en el Título IV, capítulo I, II y III del RD 1720/2007 y los siguientes artículos de la LOPD regulan su funcionamiento:

Artículo 27. Comunicación de la cesión de datos.

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

En lo relativo a la transferencia internacional de ficheros, los siguientes artículos, indicando solo aquellos puntos de las excepciones que he estimado oportunas para este caso [*trans_int*] [*transint*]: [*trans_lopd*]

Artículo 33. Norma general.

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. Excepciones.

Lo dispuesto en el artículo anterior no será de aplicación:

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

5.- Inscripción de los ficheros

El bufete tiene obligación de inscribir ciertos tipos de documentos en el Registro de la Agencia Española de Protección de Datos [*nota*]. Ficheros como "Clientes", "nóminas y personal", "usuarios de la página web", "selección de personal", "clientes potenciales y contactos" han de ser comunicados a la AEPD [*aepd*] según estipulan los artículos 25 y 26 de la LOPD y el título V, capítulo II del RD 1720/2007:

Artículo 25. Creación.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. Notificación e inscripción registral.

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

6.- Derecho de acceso a ficheros

El bufete debe habilitar un protocolo interno que garantice que tanto los empleados como los clientes puedan ejercer su Derecho ARCO de Acceso, Rectificación y Cancelación. Este derecho está amparado por los artículos 15, 16 y 17 de la LOPD y en el capítulo II (derecho de acceso), capítulo III (derechos de rectificación y cancelación) y capítulo IV (Oposición) del RD 1720/2007:

Artículo 15. Derecho de acceso.

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. Derecho de rectificación y cancelación.

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.

2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.

3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.

Cumplido el citado plazo deberá procederse a la supresión.

4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.

5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. Procedimiento de oposición, acceso, rectificación o cancelación.

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.

2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

7.- Documento de seguridad

En él figura toda la normativa de seguridad de índole técnica y organizativa necesaria para garantizar la seguridad de los datos objeto de tratamiento del bufete. Su cumplimiento será obligatorio para todo el personal que trate con documentación de carácter personal. El artículo 9 y el Título VIII, capítulo II del real decreto 1720/2007

8.- Medidas de seguridad

Las medidas de seguridad atañen tanto al entorno físico en el que está emplazado el negocio como los propios elementos de la infraestructura TI en donde se almacenan, se transmiten y se manipulan los datos que son objeto de esta ley.

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

9.- Niveles de seguridad

Dentro del ámbito de las medidas de seguridad, se definen los niveles que se le otorgan a los ficheros que maneja el bufete en función del tipo de información contenida en ellos. Estas medidas están contempladas en los siguientes artículos, en función del tipo de seguridad de dato. Dentro del RD

1720/2007 los siguientes artículos definen los principios básicos y regulan estos niveles de seguridad (básico, medio y alto).

Art. 80: niveles de seguridad:

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Art. 81: Aplicación de los niveles de seguridad:

1.- Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2.- Deberán implantarse las medidas de seguridad de nivel medio en los siguientes ficheros o tratamientos de dato de carácter personal:

- *Los relativos a la comisión de infracciones administrativas o penales*
- *Aquéllos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de Diciembre.*
- *Aquéllos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.*
- *Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.*
- *Aquéllos de los que sean responsables las entidades gestoras y servicios comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.*
- *Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.*

3.- Además de las medidas de nivel básico y medio, se aplicarán medidas de seguridad de nivel alto en los siguientes ficheros o tratamientos de datos de carácter personal:

- *Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, saluda o vida sexual.*
- *Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.*
- *Aquéllos que contengan datos derivados de actos de violencia de género.*

6.- También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado.

8.- A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

En el título I (Disposiciones Generales) – artículo 5 (definiciones) se realiza una descripción del encargado del tratamiento, sin embargo, el artículo 82 del presente capítulo realiza una descripción del ámbito de actuación de este ente (según la definición del artículo 5 puede tratarse de una persona física o jurídica, pública o privada, o de un órgano administrativo) que estimo oportuno citar a continuación.

Art. 82: encargado del tratamiento

1.- Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contentan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2.- Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenas a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3.- En todo caso, el acceso a los datos por el encargado del tratamiento estaré sometido a las medidas de seguridad contempladas en este reglamento.

La explicación detallada de las medidas de seguridad aplicables a los ficheros y tratamientos automatizados se expone en el capítulo III del presente título del RD. Los artículos relativos al nivel básico son los que van del 89 al 94, el nivel medio abarca de los artículos 95 al 100 y el nivel alto viene cubierto por los artículos 101 al 104.

Pero pese a la introducción de las TIC en los bufetes, en el negocio de la abogacía y el derecho interviene aún mucho el componente físico de los datos. Se siguen recibiendo documentación impresa en papel, los escáneres que se imprimen son escaneados y han de tratarse a posteriori como corresponda a su nivel de seguridad. Se sigue utilizando correspondencia en papel. Por lo tanto, es apropiado que se tengan en cuenta los siguientes artículos del Real Decreto 1720/2007 que se refieren a la información no automatizada descritos en el Título VIII, capítulo IV.

Sección 1ª – Medidas de seguridad de nivel básico

Artículo *105. Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.

b) Niveles de seguridad.

c) Encargado del tratamiento.

d) Prestaciones de servicios sin acceso a datos personales.

e) Delegación de autorizaciones.

f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.

g) Copias de trabajo de documentos.

h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:

a) Funciones y obligaciones del personal.

b) Registro de incidencias.

c) Control de acceso.

d) Gestión de soportes.

Artículo 106. Criterios de archivo.

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. Dispositivos de almacenamiento.

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. Custodia de los soportes.

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo

o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. Responsable de seguridad.

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. Auditoría.

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. Almacenamiento de la información.

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. Copia o reproducción.

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. Acceso a la documentación.

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.

2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.

3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. Traslado de documentación.

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

Anexo II: L.S.S.I.C.E

El presente anexo nos presenta algunos de los artículos de la L.S.S.I.C.E que se han de analizar durante el proceso de auditoría del bufete, siguiente con el proceso CObIT ME3 de cumplimiento regulatorio. El despacho dispone de una página web, que utiliza como ventana para darse a conocer a sus clientes, recabar CV de candidatos, exponer opiniones y comentarios acerca de leyes. Su función principal no es la contratación online, aunque dispone de un canal para que los posibles clientes puedan contactar, pero existen una serie de leyes que sí han de cumplir. [*lssi_gob*]

1.- Aviso Legal

Es obligatorio para cualquier página web la presencia del aviso legal en el cual se informa de los términos bajo los cuales opera el bufete. Se identifica a los responsables (nombre o denominación social, residencia, cualquier dato que permita una comunicación directa con los mencionados). Se informa del dominio, el régimen de administración en el cual se enmarca la actividad llevada a cabo por el bufete así como los datos del Colegio profesional del cual depende la profesión de la empresa. En cuyo caso, se trataría del Colegio Oficial de Abogados de Madrid y por último el número de identidad fiscal.

Sin embargo, no hay que olvidar un punto importante relativo al texto anteriormente mencionado; incluso se podría llegar a incurrir un delito relativo a los derechos de propiedad intelectual. Y es que el texto del *Aviso legal* no es tan trivial como parece. Cada empresa ha de tener el suyo propio o reproducir el texto con autorización de otra empresa. Es un detalle al que hay que prestar atención y en el cual se puede requerir los servicios de un abogado.

Este punto de la LSSI está regulado por los puntos del artículo 10 mencionados a continuación:

Artículo 10. Información general.

1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

> *a) Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.*

b) Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.

c) En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.

d) Si ejerce una profesión regulada deberá indicar:

1.º Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.

2.º El título académico oficial o profesional con el que cuente.

3.º El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.

4.º Las normas profesionales aplicables al ejercicio de su profesión y los medios a través de los cuales se puedan conocer, incluidos los electrónicos.

e) El número de identificación fiscal que le corresponda.

~~*f) Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío.*~~

g) Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.

El punto 3 de este artículo, relativo a la prestación de servicios telefónicos de tarificación adicional, no aplica a la operativa del bufete, por lo que se obvia en la mención del artículo.

2.- Política de cookies

Es obligatoria para aquellas webs que utilicen cookies no consideradas como "exentas". Existen tres tipos de cookies:

- De análisis, permiten contabilizar número de visitas, navegación por el sitio web. (*Google Analytics*)
- Técnicas: permiten la navegación y la utilización de las diferentes opciones que existan en la web (ej.: reservas)

- De personalización: permiten al usuario acceder al servicio con algunas características definidas (cookies para identificar fechas anteriormente consultadas)

En el caso del bufete las cookies empleadas serán del primer tipo, para realizar un análisis del flujo de visitas. Esto queda cubierto por el Real Decreto-Ley 13/2012, de 30 de Marzo como sigue a continuación que modifica el texto del artículo 22.2 del LSSI.

Artículo 22. Derecho de los destinatarios de servicios

> *2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*
>
> *Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones, siempre que aquél deba proceder a su configuración durante su instalación o actualización mediante una acción expresa a tal efecto.*
>
> *Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.*

3.- Comunicaciones comerciales a través de correo electrónico

El artículo 21 de la LSSI regula este proceso por el cual el bufete tiene prohibido enviar cualquier tipo de comunicación comercial sin el consentimiento de los destinatarios, sean de la naturaleza que sean. El envío de este tipo de comunicación no es justificable aludiendo a que se ha tenido acceso a los correos electrónicos de forma pública. Y por encima de todo, se ha de posibilitar que el destinatario pueda rechazar el envío de publicidad mediante la inclusión de un correo específico para este propósito. A continuación el artículo:

Artículo 21. Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.

> *1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.*

2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

Cuando las comunicaciones hubieran sido remitidas por correo electrónico, dicho medio deberá consistir necesariamente en la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección.

4.- Registro del dominio web

El registro del dominio de la página web y de todos los servicios de correo de los abogados está supeditado al artículo 9 y al segundo punto, dado que el negocio principal del bufete no está incluido en las sociedades de prestadores de servicios de la sociedad de la información.

Art. 9 – Constancia registral del nombre de dominio

~~*1. Los prestadores de servicios de la sociedad de la información establecidos en España deberán comunicar al Registro Mercantil en el que se encuentren inscritos, o a aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad, al menos, un nombre de dominio o dirección de Internet que, en su caso, utilicen para su identificación en Internet, así como todo acto de sustitución o cancelación de los mismos, salvo que dicha información conste ya en el correspondiente registro.*~~

2. Los nombres de dominio y su sustitución o cancelación se harán constar en cada registro, de conformidad con sus normas reguladoras. Las anotaciones practicadas en los Registros Mercantiles se comunicarán inmediatamente al Registro Mercantil Central para su inclusión entre los datos que son objeto de publicidad informativa por dicho Registro.

~~*3. La obligación de comunicación a que se refiere el apartado 1 deberá cumplirse en el plazo de un mes desde la obtención, sustitución o cancelación del correspondiente nombre de dominio o dirección de Internet.*~~

5.- Enlaces externos

Dentro de algunas de las secciones de la página web, existen enlaces a noticias legales, sentencias, noticias variadas, artículos legislativos de otros portales web. Para este apartado, el artículo 17 de la LSSI acerca de la responsabilidad a la hora de mencionar enlaces externos:

Art. 17 – Responsabilidad de los prestadores de servicio que faciliten enlaces a contenidos o instrumentos de búsqueda.

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o
b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

Anexo III: Glosario

CObIT: Control OBjectives for Information and related Technology (Objetivos de Control para la Información y Tecnologías relacionadas)

ITIL: Biblioteca de Infraestructura de Tecnologías de la Información (***I****nformation* ***T****echnology* ***I****nfrastructure* ***L****ibrary*)

ISACA: Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de la Información)

ITGI: IT Governance Institute (Instituto para el Control de TI)

ISACA/F: Information Systems Audit and Control Foundation (Fundación de la asociación de Auditoría y Control de Sistemas de la Información)

TI: Tecnologías de la Información:

TIC: Tecnologías de la Información y Comunicaciones

SI: Sistemas de Información:

ASI: Auditoría de Sistemas de la Información

CMMI: Capability Maturity Model Integration (Integración de modelos de madurez de capacidades)

LSSI: Ley de Servicios de Sistemas de la Información

LOPD: Ley Orgánica de Protección de Datos

SCAMPI: Standard CMMI Appraisal Method for Process Improvement

SAC: Systems Audability and Control

COSO: Committee Of Sponsoring Organizations

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

ANSI: American National Standards Institute (Instituto Nacional Estadounidense de Estándares)

PyME: Pequeña y Mediana Empresa

ISO: International Organization for Standarization (Organización Internacional de Normalización)

AEPD: Agencia Española de Protección de Datos

SAI: Sistemas de Alimentación Ininterrumpida

ARCO: Acceso, Rectificación, Cancelación y Oposición

Anexo IV: Bibliografía

[*ai_upv*] Rafael Bernal Montañés, Oscar Coltell Simón: "Auditoría de los sistema de la información" (Ed Universidad Politécnica de Valencia, servicio de publicación, 2ª ed, 2002)

[*ai_enf_pract*] Mario G. Piattini Velthuis, Emilio del Peso Navarro: "Auditoría Informática, un enfoque práctico" (Ed. Ra-Ma, 2ª ed, 2001)

[*ai_eche*] Echenique García José Antonio: "Auditoría en informática" (Ed. McGraw-Hill, 2ª ed, 2001)

[*ai_si*] Del Peso Navarro, Emilio: "Auditoría de Tecnologías y Sistemas de Información" (Ed. RA-MA, 2008)

[*trans_int*] Alvarez Riguadias, Cecilia: "Las transferencias internacionales de datos personales y el nivel equiparable o adecuado de protección" (artículo de *Uría abogados*): http://www.uria.com/documentos/publicaciones/1467/documento/art1.pdf?id=2064

Anexo V: Referencias

LO.P.D:

- [*lopd*] http://www.leyprotecciondedatos.es/
- [*aepd*] Carta de Servicios de la AEPD (formato PDF): http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/CartaServiciosAEPD.pdf
- [*lopd_pyme*] Página web de la Cámara de Comercio de Madrid en referencia a la LOPD y las Pymes: https://www.servipymelopd.es/lopd
- [*boe_lopd*] Ley Orgánica 15/1999, de 13 de Diciembre de Protección de datos de carácter personal: http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750
- [*boe_lopd_rd*] Real Decreto 1720/2007, de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de datos de carácter personal: http://www.boe.es/buscar/act.php?id=BOE-A-2008-979
- [*transint*] Regulación de transferencias de datos en el extranjero: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php
- [*trans_lopd*] Transferencia internacional de datos: http://cuidatusdatos.com/obligaciones-lopd/transferenciainternacional/index.html

L.S.S.I:

- [*lssi_gob*] Página web de Gobierno de España: http://www.lssi.gob.es/paginas/Index.aspx
- [*lssi*] Enlace a la ley 34/2002, de 11 de Julio, de Servicios de la sociedad de la información y comercio electrónico: http://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
- [*lssi_rd*] Real Decreto-Ley 13/2012, de 30 de Marzo que modifica la LSSI: http://www.minetur.gob.es/energia/es-ES/Novedades/Documents/RDL%2013_2012%20transponen%20directivas.pdf
- LSSI y Pymes: http://www.pymesyautonomos.com/tecnologia/el-aviso-legal-i-cumpliendo-con-la-lssi
- Cámara de Madrid y LSSI: http://www.camaramadrid.es/index.php?elem=305&sec=68&idsec=68

[*prop_int*] Ley de propiedad intelectual: http://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

Gobierno de TI:

- [*isaca*] Documentación acerca de ISACA y documentos con guías de auditorías: http://www.isaca.org/spanish/Pages/default.aspx
- [*metr*] Métricas: http://www.gobiernotic.es/2006/10/mtricas.html
- [cobit] Blog de Mario Saffirio – Entrada relativa a CObIT: https://msaffirio.wordpress.com/2007/03/03/la-cobit-y-la-organizacion-del-area-informatica/
- [*nota*] Inscripción de ficheros en sistema NOTA: http://www.ayudaleyproteccionda-tos.es/2015/07/09/como-inscribir-ficheros-con-el-nuevo-sistema-nota/
- [*itil*] BITCompany – Gobierno de ITIL con CObIT: http://www.bitcompany.biz/gobierno-corporativo-de-it-itil-o-cobit/#.VhFwn5Xou02
- [*gobti_norm*] Gobierno TI normalizado: http://gestionproyectos.260mb.net/?ckattempt=1
- [*gobTI_ieee*] Metodologías y Normas para gobierno TI – IEEE: http://sites.ieee.org/spain-tmc/2011/07/30/metodologias-y-normas-para-gobierno-de-ti-2/
- [*iso20000*] Norma UNE_ISO/IEC 20000 – Web Aenor: http://www.aenor.es/aenor/certificacion/calidad/calidad_serviciosti_20000.asp

- [*cob41*] Cobit 4.1 en ISACA: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

La PYME y las TIC en España:

- [*pyme15*] Retrato de las PYME en España en 2015: http://www.ipyme.org/Publicaciones/Retrato_PYME_2015.pdf
- [*ontsi*] Estudio "Análisis sectorial de la implantación de las TIC en la PYME Española" del ONTSI: http://www.ontsi.red.es/ontsi/es/estudios-informes/e-pyme-14-an%C3%A1lisis-sectorial-de-implantaci%C3%B3n-de-las-tic-en-la-pyme-espa%C3%B1ola
- [*epyme14*] Informe epyme 2014: http://www.ipyme.org/Publicaciones/informe-epyme-2014.pdf
- [*artmun*] Artículo "¿Somos una economía digital? En España 1 de cada 3 empresas no tiene ordenador ni internet" de El Mundo: http://www.elmundo.es/economia/2015/07/07/559aafcf22601d435c8b45a4.html